OS/390

Security Server (RACF) Planning: Installation and Migration

GC28-1920-03

OS/390

Security Server (RACF) Planning: Installation and Migration

GC28-1920-03

Note

Before using this information and the product it supports, be sure to read the general information under “Notices” on page vii.

Fourth Edition, September 1997

This is a major revision of GC28-1920-02.

This edition applies to Version 2 Release 4 of OS/390 (5647-A01) and to all subsequent releases and modifications until otherwise indicated in new editions.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address below.

IBM welcomes your comments. A form for readers' comments may be provided at the back of this publication, or you may address your comments to the following address:

International Business Machines Corporation
Department 55JA, Mail Station P384
522 South Road
Poughkeepsie, NY 12601-5400
United States of America

FAX (United States & Canada): 1+914+432-9405
FAX (Other Countries):
Your International Access Code +1+914+432-9405

IBMLink (United States customers only): KGNVMC(MHVRCFS)
IBM Mail Exchange: USIB6TC9 at IBMMAIL
Internet e-mail: mhvrcfs@vnet.ibm.com
World Wide Web: http://www.s390.ibm.com/os390

If you would like a reply, be sure to include your name, address, telephone number, or FAX number.

Make sure to include the following in your comment or note:

- Title and order number of this book
- Page number or topic related to your comment

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© **Copyright International Business Machines Corporation 1994, 1997. All rights reserved.**
Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

Notices vii

Trademarks ix

About This Book xi
Who Should Use This Book xi
How to Use This Book xi
Where to Find More Information xii
IBM Systems Center Publications xiii
Other Sources of Information xiv
To Request Copies of IBM Publications xv

Summary of Changes xvii

Chapter 1. Planning for Migration 1
Migration Planning Considerations 1
Installation Considerations 2
Customization Considerations 2
Administration Considerations 2
Auditing Considerations 3
Application Development Considerations 3
General User Considerations 3

Chapter 2. Release Overview 5
New and Enhanced Support 5
RACF/DB2 External Security Module 5
Enhancements to Support for OpenEdition Services 6
Run-Time Library Services 7
Password History Enhancements 7
Tivoli Management Environment (TME) 10 Global Enterprise Management User Administration Service 8
Program Control by System ID 8
New FMID 9
OW24966 Enhancements to TARGET Command 9
Enable/Disable Changes 10
OW26237 Enhancements of Global Access Checking 10

Chapter 3. Summary of Changes to RACF Components for OS/390 Release 4 11
Callable Services 11
Class Descriptor Table (CDT) 12
Commands 13
Data Areas 15
Exits 16
Macros 17
Messages 17
New Messages 17
Changed Messages 17
Deleted Messages 18
Panels 18

© Copyright IBM Corp. 1994, 1997

SYS1.SAMPLIB 19
Publications Library 20

Chapter 4. Planning Considerations 21
Migration Strategy 21
Migration Paths for OS/390 Release 4 Security Server (RACF) 21
Hardware Requirements 22
Compatibility 23
OpenEdition MVS 23
Program Control by System ID 23
RELEASE=2.4 Keyword on Macros 23

Chapter 5. Installation Considerations 25
RACF Storage Considerations 25
Virtual Storage 25
Templates for RACF on OS/390 Release 4 27

Chapter 6. Customization Considerations 29
Customer Additions to the Router Table and the CDT 29
RACF/DB2 External Security Module Customization 29
Exit Processing 30

Chapter 7. Administration Considerations 31
The TMEADMIN Class 31
Password History Changes 31
Program Control by System ID 31
Enhancements of Global Access Checking 32

Chapter 8. Auditing Considerations 33
SMF Records 33

Chapter 9. Application Development Considerations 35
Programming Interfaces 35
RELEASE=2.4 Keyword on Macros 35
FASTAUTH Changes 35

Chapter 10. General User Considerations 37
Password History Changes 37

Glossary 39

How to Get Your RACF CD 47

Index 49

Figures

1. New Callable Services 11
2. Changed Callable Services 12
3. New Classes 13
4. Changes to RACF Commands 13
5. Changes to PSPI Data Areas 16
6. Changed Executable Macros 17
7. New Panels for RACF 19
8. Changed Panels for RACF 19
9. Change to SYS1.SAMPLIB 19
10. Changes to the RACF Publications Library 20
11. RACF Estimated Storage Usage 25
12. Changes to SMF Records 33

© Copyright IBM Corp. 1994, 1997

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates.

Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. A functionally equivalent product, program, or service which does not infringe on any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, programs, or services, except those expressly designated by IBM, is the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
USA

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Mail Station P300
522 South Road
Poughkeepsie, NY 12601-5400
USA
Attention: Information Request

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

© Copyright IBM Corp. 1994, 1997

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

- AIX/6000
- BookManager
- CICS
- CICS/ESA
- DB2
- DFSMS
- FFST
- FFST/MVS
- IBM
- IBMLink
- IMS
- Library Reader
- MVS/ESA
- MVS/XA
- NetView
- OpenEdition
- OS/2
- OS/390
- Parallel Sysplex
- RACF
- RETAIN
- S/390
- SOMobjects
- System/390
- SystemView
- TalkLink
- VM/ESA
- VM/XA

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Windows is a trademark of Microsoft Corporation.

Other company, product, and service names, which may be denoted by a double asterisk (**), may be trademarks or service marks of others.

© Copyright IBM Corp. 1994, 1997

About This Book

This book contains information about the Resource Access Control Facility (RACF), which is part of the OS/390 Security Server. The Security Server has two components:

- RACF
- OpenEdition DCE Security Server

For information about the OpenEdition DCE Security Server, see the publications related to that component.

This book provides information to guide you through the migration process from OS/390 Release 3 Security Server (RACF) or RACF to OS/390 Release 4 Security Server (RACF).

The purpose of this book is to ensure an orderly transition to a new RACF release. It is *not* intended for customers installing RACF for the first time or installing a release prior to Security Server (RACF) Release 3. First-time RACF customers should read *OS/390 Security Server (RACF) Introduction* and use the program directory shipped with the product when they are ready to install the product.

Who Should Use This Book

This book is intended for experienced system programmers responsible for migrating from OS/390 Release 3 Security Server (RACF) to OS/390 Release 4 Security Server (RACF). This book assumes you have knowledge of OS/390 Release 3 Security Server (RACF).

If you are migrating from a RACF 2.2, or earlier, or from an OS/390 Security Server release prior to OS/390 Release 3, you should also read previous versions of this book, as described in “Migration Paths for OS/390 Release 4 Security Server (RACF)” on page 21.

How to Use This Book

This book is organized in the following order:

- Chapter 1, “Planning for Migration” on page 1, provides information to help you plan your installation's migration to the new release of RACF.
- Chapter 2, “Release Overview” on page 5, provides an overview of support in the new release.
- Chapter 3, “Summary of Changes to RACF Components for OS/390 Release 4” on page 11, lists specific new and changed support for the new release.
- Chapter 4, “Planning Considerations” on page 21, describes high-level migration considerations for customers upgrading to the new release of RACF from previous levels of RACF.
- Chapter 5, “Installation Considerations” on page 25, highlights information about installing the new release of RACF.

© Copyright IBM Corp. 1994, 1997

- Chapter 6, “Customization Considerations” on page 29, highlights information about customizing function to take advantage of new support after the new release of RACF is installed.
- Chapter 7, “Administration Considerations” on page 31, summarizes changes to administration procedures for the new release of RACF.
- Chapter 8, “Auditing Considerations” on page 33, summarizes changes to auditing procedures for the new release of RACF.
- Chapter 9, “Application Development Considerations” on page 35, identifies changes in the new release of RACF that might require changes to an installation's existing programs.
- Chapter 10, “General User Considerations” on page 37, summarizes new support that might affect general user procedures.

Where to Find More Information

Where necessary, this book references information in other books. For complete titles and order numbers for all products that are part of OS/390, see *OS/390 Information Roadmap*.

Softcopy Publications

The OS/390 Security Server (RACF) library is available on the following CD-ROMs. The CD-ROM collections include the IBM Library Reader, a program that enables customers to read the softcopy books.

- The *OS/390 Security Server (RACF) Information Package*, SK2T-2180

  This softcopy collection kit contains the OS/390 Security Server (RACF) library. It also contains the RACF/MVS Version 2 product libraries, the RACF/VM 1.10 product library, product books from the OS/390 and VM collections, International Technical Support Organization (ITSO) books, and Washington System Center (WSC) books that contain substantial amounts of information related to RACF. The kit does not contain any licensed publications. By using this CD-ROM, you have access to RACF-related information from IBM products such as OS/390, VM, CICS, and NetView without maintaining shelves of hardcopy documentation or handling multiple CD-ROMs. To get more information on the *OS/390 Security Server (RACF) Information Package*, see the advertisement at the back of the book.

- The *OS/390 Collection Kit*, SK2T-6700

  This softcopy collection contains a set of OS/390 and related product books. This kit contains unlicensed books.

- The *Online Library Omnibus Edition MVS Collection Kit,* SK2T-0710

  This softcopy collection contains a set of key MVS and MVS-related product books. It also includes the RACF Version 2 product libraries. *OS/390 Security Server (RACF) Messages and Codes* is also available as part of *Online Library Productivity Edition Messages and Codes Collection,* SK2T-2068.

RACF Courses

The following RACF classroom courses are also available:

- *Effective RACF Administration,* H3927
- *MVS/ESA RACF Security Topics,* H3918
- *Implementing RACF Security for CICS/ESA,* H3992

IBM provides a variety of educational offerings for RACF. For more information on classroom courses and other offerings, see your IBM representative, *IBM Mainframe Training Solutions*, GR28-5467, or call 1-800-IBM-TEACH (1-800-426-8322).

IBM Systems Center Publications

IBM systems centers produce “red” and “orange” books that can be helpful in setting up and using RACF.

These books have not been subjected to any formal review nor have they been checked for technical accuracy, but they represent current product understanding (at the time of their publication) and provide valuable information on a wide range of RACF topics. They are not shipped with RACF. You must order them separately. A selected list of these books follows:

- *Systems Security Publications Bibliography,* G320-9279
- *Elements of Security: RACF Overview - Student Notes,* GG24-3970
- *Elements of Security: RACF Installation - Student Notes,* GG24-3971
- *Elements of Security: RACF Advanced Topics - Student Notes,* GG24-3972
- *RACF Version 2 Release 2 Technical Presentation Guide,* GG24-2539
- *RACF Version 2 Release 2 Installation and Implementation Guide,* SG24-4580
- *Enhanced Auditing Using the RACF SMF Data Unload Utility,* GG24-4453
- *RACF Macros and Exit Coding,* GG24-3984
- *RACF Support for Open Systems Technical Presentation Guide,* GG26-2005
- *DFSMS and RACF Usage Considerations,* GG24-3378
- *Introduction to System and Network Security: Considerations, Options, and Techniques,* GG24-3451
- *Network Security Involving the NetView Family of Products,* GG24-3524
- *System/390 MVS Sysplex Hardware and Software Migration,* GC28-1210
- *Secured Single Signon in a Client/Server Environment,* GG24-4282
- *Tutorial: Options for Tuning RACF,* GG22-9396
- *OS/390 Security Server Audit Tool and Report Application*, SG24-4820

Other books are available, but they are not included in this list, either because the information they present has been incorporated into IBM product manuals, or because their technical content is outdated.

Other Sources of Information

IBM provides customer-accessible discussion areas where RACF may be discussed by customer and IBM participants. Other information is available through the Internet.

IBM Discussion Areas

Two discussion areas provided by IBM are the MVSRACF discussion and the SECURITY discussion.

- **MVSRACF**

  MVSRACF is available to customers through IBM's TalkLink offering. To access MVSRACF from TalkLink:

  1. Select S390 (the S/390 Developers' Association).
  2. Use the fastpath keyword: MVSRACF.

- **SECURITY**

  SECURITY is available to customers through IBM's DialIBM offering, which may be known by other names in various countries. To access SECURITY:

  1. Use the CONFER fastpath option.
  2. Select the SECURITY CFORUM.

Contact your IBM representative for information on TalkLink, DialIBM, or equivalent offerings for your country and for more information on the availability of the MVSRACF and SECURITY discussions.

Internet Sources

The following resources are available through the Internet:

- **RACF home page**

  You can visit the RACF home page on the World Wide Web using this address:

  http://www.s390.ibm.com/products/racf/racfhp.html

  or

  http://www.s390.ibm.com/racf

- **RACF-L discussion list**

  Customers and IBM participants may also discuss RACF on the RACF-L discussion list. RACF-L is not operated or sponsored by IBM; it is run by the University of Georgia.

  To subscribe to the RACF-L discussion, so you can receive postings, send a note to:

  listserv@uga.cc.uga.edu

  Include the following line in the body of the note, substituting your first name and last name as indicated:

  subscribe racf-l *first_name last_name*

  To post a question or response to RACF-L, send a note to:

  racf-l@uga.cc.uga.edu

  Include an appropriate `Subject:` line.

- **Sample code**

You can get sample code, internally-developed tools, and exits to help you use RACF. All this code works in our environment, at the time we make it available, but is not officially supported. Each tool or sample has a README file that describes the tool or sample and any restrictions on its use.

The simplest way to reach this code is through the RACF home page. From the home page, click on **System/390 FTP Servers** under the topic, "RACF Sample Materials."

The code is also available from **lscftp.pok.ibm.com** through **anonymous ftp**.

To get access:

1. Log in as user **anonymous**.
2. Change the directory (**cd**) to **/pub/racf/mvs** to find the subdirectories that contain the sample code. We'll post an announcement on RACF-L, MVSRACF, and SECURITY CFORUM whenever we add anything.

Restrictions

Because the sample code and tools are not officially supported,

- There are no guaranteed enhancements.
- No APARs can be accepted.

The name and availability of the **ftp** server may change in the future. We'll post an announcement on RACF-L, MVSRACF, and SECURITY CFORUM if this happens.

However, even with these restrictions, it should be useful for you to have access to this code.

To Request Copies of IBM Publications

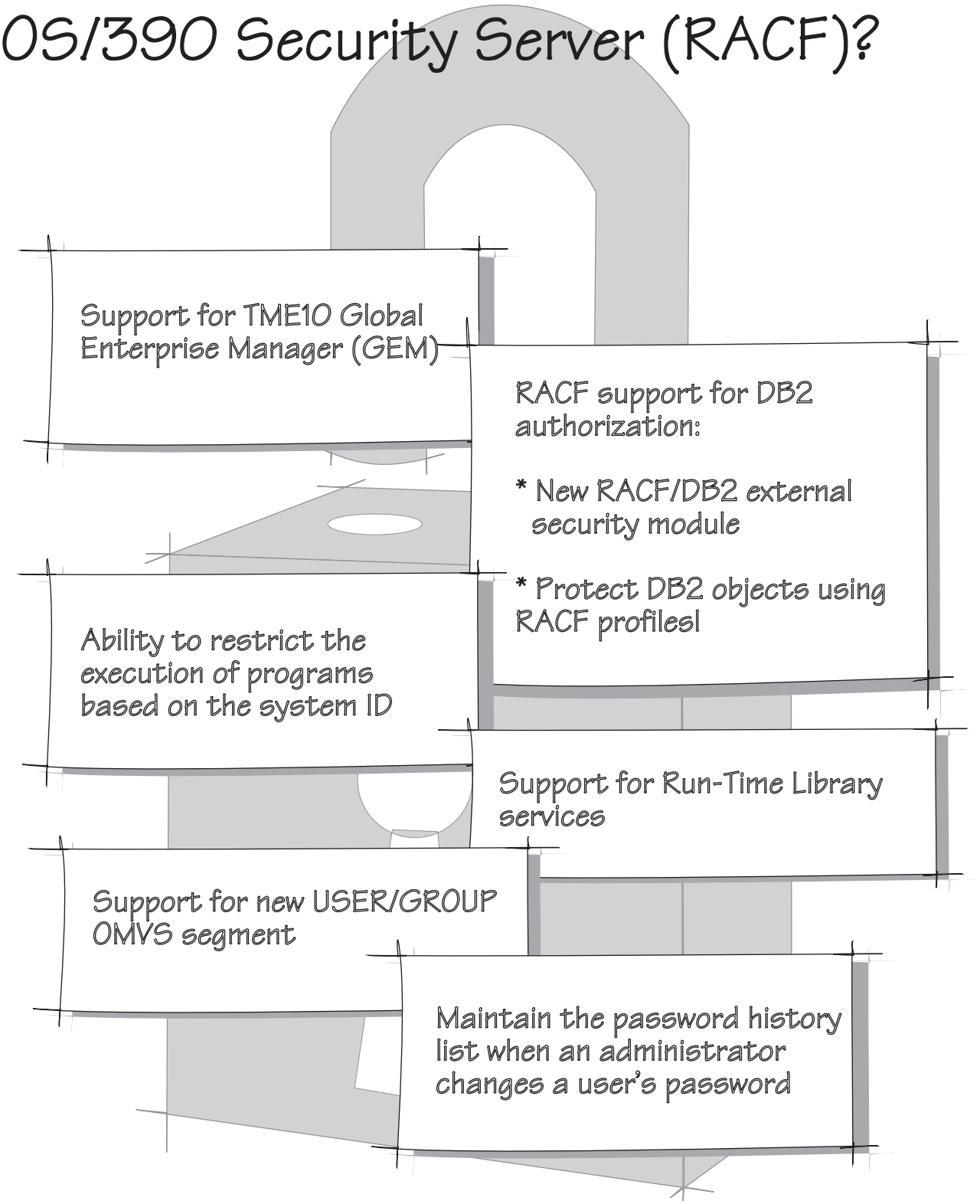
Direct your request for copies of any IBM publication to your IBM representative or to the IBM branch office serving your locality.

There is also a toll-free customer support number (1-800-879-2755) available Monday through Friday from 6:30 a.m. through 5:00 p.m. Mountain Time. You can use this number to:

- Order or inquire about IBM publications
- Resolve any software manufacturing or delivery concerns
- Activate the Program Reorder Form to provide faster and more convenient ordering of software updates

See the advertisement at the back of the book for information about the *OS/390 Security Server (RACF) Information Package.*

What's New in Release 4 for OS/390 Security Server (RACF)?



Summary of Changes

Summary of Changes
for GC28-1920-03
OS/390 Version 2 Release 4

This book contains primarily new information for OS/390 Version 2 Release 4 Security Server (RACF). When any information appeared in an earlier release, the information that is new is indicated by a vertical line to the left of the change.

Summary of Changes
for GC28-1920-02
OS/390 Release 3

This book contains new information for OS/390 Release 3 Security Server (RACF).

Summary of Changes
for GC28-1920-01
OS/390 Release 2

This book contains new information for OS/390 Release 2 Security Server (RACF).

Summary of Changes
for GC28-1920-00
OS/390 Release 1

This book contains information previously presented in *RACF Planning: Installation and Migration*, GC23-3736, which supports RACF Version 2 Release 2.

This book includes terminology, maintenance, and editorial changes.

© Copyright IBM Corp. 1994, 1997

Chapter 1. Planning for Migration

This chapter provides information to help you plan your installation's migration to the new release of OS/390 Security Server (RACF). Before attempting to migrate, you should define a plan to ensure a smooth and orderly transition. A well thought-out and documented migration plan can help minimize any interruption of service. Your migration plan should address such topics as:

- Identifying which required and optional products are needed
- Evaluating new and changed functions
- Evaluating how incompatibilities affect your installation
- Defining necessary changes to:
  - Installation-written code
  - Operational procedures
  - Application programs
  - Other related products
- Defining education requirements for operators and end users
- Preparing your staff and end users for migration, if necessary
- Acquiring and installing the latest service level of RACF for maintenance

The content and extent of a migration plan can vary significantly from installation to installation. To successfully migrate to a new release of RACF, you should start by installing and stabilizing the new RACF release without activating the new functions provided. Installing the new RACF release without initially exploiting new functions allows you to maintain a stable RACF environment. The program directory shipped with the new OS/390 release gives detailed information about the correct software required for installation.

When defining your installation's migration plan, you should consider the following:

- Migration
- Installation
- Customization
- Administration
- Auditing
- Operation
- Application development
- General users

Migration Planning Considerations

Installations planning to migrate to a new release of RACF must consider high-level support requirements such as machine and programming restrictions, migration paths, and program compatibility.

For more information, see Chapter 4, “Planning Considerations” on page 21.

© Copyright IBM Corp. 1994, 1997

Installation Considerations

Before installing a new release of RACF, you must determine what updates are needed for IBM-supplied products, system libraries, and non-IBM products. (Procedures for installing RACF are described in the program directory shipped with OS/390, not in this book.)

Be sure you include the following steps when planning your pre-installation activities:

- Obtain and install any required program temporary fixes (PTFs) or updated versions of the operating system.

  Call the IBM Software Support Center to obtain the preventive service planning (PSP) upgrade for RACF. This provides the most current information on PTFs for RACF. Have RETAIN checked again just before testing RACF. Information for requesting the PSP upgrade can be found in the program directory. Although the program directory contains a list of the required PTFs, the most current information is available from the support center.

- Contact programmers responsible for updating programs.

  Verify that your installation's programs will continue to run, and, if necessary, make changes to ensure compatibility with the new release.

For more information, see Chapter 5, “Installation Considerations” on page 25.

Customization Considerations

In order for RACF to meet the specific requirements of your installation, you can customize function to take advantage of new support after the product is installed. For example, you can tailor RACF through the use of installation exit routines, class descriptor table (CDT) support, or options to improve performance. This book lists changes to RACF that might require the installation to tailor the product, either to ensure that RACF runs as before or to accommodate new security controls that an installation requires.

For more information, see Chapter 6, “Customization Considerations” on page 29.

Administration Considerations

Security administrators must be aware of how changes introduced by a new product release can affect an installation's data processing resources. Changes to real and virtual storage requirements, performance, security, and integrity are of interest to security administrators or to system programmers who are responsible for making decisions about the computing system resources used with a program.

For more information, see Chapter 7, “Administration Considerations” on page 31.

Auditing Considerations

Auditors who are responsible for ensuring proper access control and accountability for their installation are interested in changes to security options, audit records, and report generation utilities.

For more information, see Chapter 8, “Auditing Considerations” on page 33.

Application Development Considerations

Application development programmers must be aware of new functions introduced in a new release of RACF. To implement a new function, the application development personnel should read this book and the following books:

- *OS/390 Security Server External Security Interface (RACROUTE) Macro Reference*
- *OS/390 Security Server (RACF) Data Areas*
- *OS/390 Security Server (RACF) Macros and Interfaces*

To ensure that existing programs run as before, the application programmers should be aware of any changes in data areas and processing requirements. This book provides an overview of the changes that might affect existing application programs.

For more information, see Chapter 9, “Application Development Considerations” on page 35.

General User Considerations

RACF general users use a RACF-protected system to:

- Log on to the system
- Access resources on the system
- Protect their own resources and any group resources to which they have administrative authority

This book provides an overview of the changes that might affect existing procedures for general users. For more information, see Chapter 10, “General User Considerations” on page 37.

Chapter 2. Release Overview

This chapter lists the new and enhanced functions of RACF for OS/390 Release 4 and gives a brief overview of each new function or function enhancement.

New and Enhanced Support

For OS/390 Release 4, RACF provides:

- Support for the RACF/DB2 external security module
- Additional auditing of OpenEdition superusers status
- Default OpenEdition USER/GROUP support
- Run-time library services support
- Password history enhancements
- OW23445 enhancement to allow RACF user profile administration using Tivoli Management Environment (TME) administration service
- OW25727 enhancement to allow program control by system ID
- New FMID
- OW24966 enhancements to TARGET command
- Enable/disable changes
- OW26237 enhancements to global access checking

RACF/DB2 External Security Module

The Security Server for OS/390 Release 4 is providing a new function that gives you the ability to control access to DB2 objects using RACF profiles. This function is provided as a fully supported exit module called the RACF/DB2 external security module. If you choose to use this new support, the module is designed to receive control from the DB2 access control authorization exit point. The highlights of the support include:

- Single point of control for administering and auditing DB2 access
- Ability to define security rules before a DB2 object is created
- Ability to have security rules persist when a DB2 object is dropped
- Ability to control access to DB2 objects with generic profiles
- Flexibility to control access to DB2 objects for single or multiple subsystems with a single set of RACF profiles
- Ability to validate a user ID before permitting it access to a DB2 object
- Elimination of DB2 cascading revoke

Use of this function requires the DB2 access control authorization exit point function provided in DB2 Version 5.

© Copyright IBM Corp. 1994, 1997

Enhancements to Support for OpenEdition Services

Enhancements to RACF's support for OpenEdition services include:

- Extended ability to audit the use of superuser status
- Default USER/GROUP support provided by APAR OW26800

Extended Ability to Audit the Use of Superuser Status

This support allows the auditing of the new OpenEdition spawn service. It determines when a user is a superuser and the identity of that user. This extended audit function allows a full audit trail that can be used to ensure that security is adequate.

Auditing the use of superuser status is performed using the ck_priv event code and the PROCESS class processing to audit UID and GID changes. The audit function code 101 is added.

If you are not already auditing the PROCESS class, issue SETROPTS LOGOPTIONS(xxxx(PROCESS)) to obtain the SMF TYPE80 record ck_priv.

Default USER/GROUP OMVS Segment Provided by APAR OW26800

RACF allows definition of a system-wide default for OMVS segment information, making it possible for users not specifically defined OpenEdition MVS users to make use of OpenEdition services.

With this release, OpenEdition sockets are the primary socket interface . To utilize this support, RACF provides the ability to define default OpenEdition information by setting a system-wide option.

Previously, to use OpenEdition services, you needed to have a RACF USER profile with an OMVS segment containing a UID and a current connect group that had a GROUP profile with an OMVS segment containing a GID. If these were not available, the initUSP service failed and the process could not use OpenEdition services.

Now, if no OMVS segment is found in the USER profile during initUSP processing, the default OMVS segment is used. If the default is found, it is used to set the UID, HOME, and PROGRAM values for the user. If no default value is found, the initUSP fails with the existing RACF return code of 8 and reason code of 20.

The same processing is done for the user's current connect group. If no OMVS segment is found in the GROUP profile, the default is used. If no default value is found, the initUSP fails with the existing RACF return code of 8 and reason code of 8.

After a default UID, GID, or both are assigned, initUSP processing continues. If the user is connected to additional RACF groups and list-of-groups processing is active, the supplemental group list is built using the GIDs of these additional groups. No default processing occurs while the supplemental group list is built.

When initUSP assigns a default UID, GID, or both, it sets a bit in the user's USP to indicate that it is a default USP. This bit causes an additional relocate section to be added to any SMF TYPE80 records written by RACF callable services for this user.

The getUMAP and getGMAP services also look for default values. If getUMAP is given a UID as input and the corresponding USER profile has no OMVS segment, the caller of the getUMAP service receives the default. If no default value is found, RACF return code 8, reason code 4 are returned by the getUMAP service. If a UID is passed to getUMAP, then it returns a user ID, which is likely to return the user ID of the default user.

Similarly, if getGMAP is given a GID as input and the corresponding GROUP profile has no OMVS segment, the caller of the getGMAP service receives the default. If no default value is found, RACF return code 8, reason code 4 are returned by the getGMAP service. If a GID is passed to getGMAP, it returns a group name, which is likely to return the group name of the default group.

The default OMVS segments reside in a USER profile and a GROUP profile. The installation selects the names of these profiles, using a profile in the FACILITY class. The name of the FACILITY class profile is BPX.DEFAULT.USER. The application data field contains the user ID and the group name. The user profile for the user ID specified contains the UID, and the group profile for the group name specified contains the GID.

In order to use this default USER/GROUP support, the following need to be done:

- Make the FACILITY class active.
- Define BPX.DEFAULT.USER with APPLDATA('*uuuu/gggg*') where *uuuu* specifies a default user ID of 1-8 characters and *gggg* specifies a default group name of 1-8 characters. The USER profile *uuuu* needs to have an OMVS segment with the default UID, HOME, and PROGRAM. The GROUP profile *gggg* needs to have an OMVS segment giving the default GID.
- If only default user information is needed, use APPLDATA ('*uuuu*').

The processing of the default OMVS segments for the user and the current connection group are independent of each other. The OMVS segment of the user specified on the initUSP may be used to obtain the UID, and the user may come from the group ID specified in the FACILITY class profile. Similarly, when the default UID found through the user ID specified in the FACILITY class profile is used, the GID may come from the user's current connect group. Also the user specified in the FACILITY class profile does not need to be a member of the group specified in that profile. These values are used independently.

Run-Time Library Services

The Run-Time Library Services (RTLS) of OS/390 introduce new contents supervisor support to facilitate the binding of applications to a specific language run-time environment defined on an installation basis. System programmers can use FACILITY class profiles and RACF's program control when there is a need to control access to run-time libraries and the programs that use the run-time libraries.

Password History Enhancements

The password history enhancement makes it easier for installations to prevent end users from circumventing password history security policy. The old password is saved in the password history list when a password is reset by an administrator.

The following commands have been modified to save the old password whenever the password is reset:

- The ALTUSER command allows an administrator to reset a user's password to a temporary password or a default value. This command is modified to save the old password whenever the password is reset.
- The PASSWORD USER (*userid*) command provides users and administrators with a password reset function. This command is modified to save the old password whenever the password is reset.

Tivoli Management Environment (TME) 10 Global Enterprise Management User Administration Service

The Tivoli Management Environment (TME) 10 Global Enterprise Manager User Administration Service provides the ability to manage UNIX, Windows NT, NetWare, and RACF accounts from a single, common interface (either graphical or command line). The RACF support for this, which was provided by APARs OW23445 and OW23446, includes:

The TMEADMIN class, which is used to map a TME administrator to a RACF user ID.

Callable services to:

- Derive a session key from a previously generated RACF PassTicket. The Tivoli Management Region (TMR) TCP/IP server uses such session keys to encrypt and decrypt administrative data that flows between the TMR server and OS/390.
- Convey RACF administrative changes to RACF. The new R_Admin callable service provides a function-code driven parameter list with data fields consisting of name-value pairs. This name-value pair support is used by the TME user administration service to add or update the following RACF user profile information:
  - BASE profile information
  - OMVS segment
  - NETVIEW segment
  - TSO segment
  - CICS segment

In addition to the above, the R_Admin callable service provides a run command function in which most RACF TSO commands may be executed.

Changes to the RACF TSO command ALTUSER. The NOCLAUTH key will now accept an asterisk ('*') to indicate removal of all of the user's CLAUTH authorities.

Program Control by System ID

RACF provides a means to restrict access to a program based on the system identifier (SMFID). This additional program control by system ID improves system management and usability of program products in a sysplex environment. It also eliminates error-prone manual procedures, the need to keep DASD that is not shared, and the potential savings on licensing fees by controlling which systems in a sysplex the licensed software may execute on. Previously many customers complied with licensing agreements by paying for ALL system that the software COULD run on because there was no easy way to restrict access to a particular

system. This support provides a solution to many customers that find themselves in such a situation.

The PERMIT command has a new keyword to add users and groups to the conditional access list, WHEN(SYSID(...)). This keyword is allowed only for the PROGRAM class. WHEN(SYSID(...)) is similar to the existing keywords WHEN(TERMINAL(...)), WHEN(PROGRAM(...)), and WHEN(JESINPUT(...)). No class is associated with SYSID. In addition, no check is made to determine whether the value specified for SYSID is valid.

A new error message is issued if WHEN(SYSID(...)) is specified for a class other than PROGRAM. When copying a conditional access list from a PROGRAM profile to a non-PROGRAM profile, WHEN(SYSID(...)) entries are not copied. No messages are issued if this is the case. This applies to ADDSD FROM, RDEFINE FROM, RACROUTE REQUEST=DEFINE with modeling, and PERMIT FROM.

New FMID

OS/390 Release 4 Security Server (RACF) has a new FMID, HRF2240. Although RACF, as a component of the OS/390 Security Server, no longer has a version, release, and modification level of its own, for compatibility with previous versions and releases of RACF the new FMID is treated as if it represented version 2.4.0. The RCVT contains the value 2040 to identify the RACF level. The ICHEINTY, ICHEACTN, and ICHETEST macros accept the keyword RELEASE=2.4, although they support no new keywords that would require the RELEASE=2.4 keyword.

OW24966 Enhancements to TARGET Command

The RACF TARGET command now accepts the new keyword WDSQUAL to allow allocation of the work space data sets when the system name starts with a numeric character. This keyword indicates that the variable that follows is the middle qualifier used by RRSF for the workspace data set qualifier names of the INMSG and OUTMSG queues for the local RRSF node defined by the TARGET command. WDSQUAL cannot be used for a remote node.

The format for the qualified name is *prefix.wdsqual. ds_identity*. *wdsqual* can be from 1 to 8 characters long beginning with an alphabetic character. Initial numerals are not accepted. The formation of the workspace data set names can be changed until the data sets are allocated. Specifying WDSQUAL on another TARGET command after its node has become dormant or operative is not allowed. Specifying of WDSQUAL on the same command is allowed.

If you have any TARGET commands in your IRROPTxx RACF parameter library member that specify the WORKSPACE keyword abbreviated to a W, you need to increase the length of that keyword to at least WO so it is not mistaken for the new WDSQUAL keyword which is now represented as W. It is recommended that the use of abbreviations be avoided in clists, REXX execs, and parmlib statements.

If WDSQUAL is not specified, the previously used format for the data set names is used. This is *prefix.sysname*.INMSG and *prefix.sysname*.OUTMSG.

For more information on the TARGET command, see *OS/390 Security Server (RACF) Command Language Reference*.

Enable/Disable Changes

OS/390 Version 2 Release 4 has a new product ID that affects the enable/disable function in all of its elements including the Security Server. The ID() value used in the IFAPRDxx parmlib member needs to be "5647-A01". The remainder of the parameters remain the same. Without this necessary change to the ID() parameter, the Security Server will not initialize. In order to keep from making changes in the future, you can use the value ID(*). For more information, see *OS/390 Security Server (RACF) System Programmer's Guide*.

OW26237 Enhancements of Global Access Checking

This enhancement allows RACROUTE REQUEST=AUTH processing to use global access checking for general resource classes regardless of whether or not the class has been RACLISTed by either SETROPTS RACLIST or RACROUTE REQUEST=LIST. Authorization checking using RACROUTE REQUEST=AUTH searches the global access checking table for a matching entry, ignoring profiles in the class. If no global access checking table entry matches the search, or if the access specified in the entry is less than the access being requested, RACF then searches for a matching profile in the class. With this release of OS/390 Security Server (RACF), this processing occurs regardless of whether or not the class is RACLISTed using SETROPTS RACLIST or RACROUTE REQUEST=LIST.

Chapter 3. Summary of Changes to RACF Components for OS/390 Release 4

This chapter summarizes the new and changed components of OS/390 Release 4 Security Server (RACF). It includes the following summary charts for changes to the RACF:

- Callable Services
- Class descriptor table (CDT)
- Commands
- Data Areas
- Exits
- Macros
- Messages
- Panels
- SYS1.SAMPLIB
- Publications Library

Callable Services

Figure 1 lists a new callable service. This callable service is a PSPI attachment interface, which means that it is not intended for use in customer application programs, but rather for use by other IBM components or vendor programs.

Figure 1. New Callable Services

Callable Service Name	Description	Support
R_admin	The R_admin service enables applications to manage RACF user profiles within the RACF database.This service accepts either a function code-driven parameter list with data fields consisting of name-value pairs or a preconstructed RACF TSO command to be executed. R_admin does NOT include the following RACF commands: BLKUPD, RVARY, RACLINK. It also does NOT include RACF operator commands such as DISPLAY, RESTART, SET, SIGNOFF, STOP, and TARGET.	TME 10

© Copyright IBM Corp. 1994, 1997

Figure 2. Changed Callable Services

Callable Service Name	Description	Support
initUSP	• If no OMVS segment is found in the user's profile, the initUSP service checks the BPX.DEFAULT.USER profile in the FACILITY class. This profile may contain a user ID in its application data field that provides a default OMVS segment. If this default is found, it is used to set the UID, HOME, and PROGRAM for the user. • If no OMVS segment is found in the group profile of the user's current connect group, the initUSP service checks the BPX.DEFAULT.USER profile in the FACILITY class. This profile may contain a group ID in the application data field that provides a default OMVS segment. If this default is found, it is used to set the GID for the user. • If any defaults are used by initUSP, a bit is set in the resulting USP to indicate that this is the default Open Edition security environment. Any audit records written by subsequent RACF callable services reflect this.	Default USER/GROUP OMVS Segment
getGMAP	• If getGMAP is given a group ID as input and the corresponding GROUP profile has no OMVS segment, getGMAP checks the BPX.DEFAULT.USER profile in the FACILITY class. This profile may contain a group ID in its application data field that provides a default OMVS segment. If this default is found, its GID is returned to the issuer of getGMAP.	Default USER/GROUP OMVS Segment
getUMAP	• If getUMAP is given a user ID as input and the corresponding USER profile has no OMVS segment, getUMAP checks the BPX.DEFAULT.USER profile in the FACILITY class. This profile may contain a user ID in its application data field that provides a default OMVS segment. If this default is found, its UID is returned to the issuer of getUMAP.	Default USER/GROUP OMVS Segment

Class Descriptor Table (CDT)

Figure 3 lists new classes provided in the IBM-supplied class descriptor table (ICHRRCDX). The class names are general-use programming interfaces (GUPI) for ICHEINTY and RACROUTE. There is a set of entries corresponding to the new classes added in the IBM-supplied router tables.

Figure 3. New Classes

Name	Description	Support
DSNADM	DB2 administrative authority class	DB2
GDSNBP	Grouping class for buffer pool privileges	DB2
GDSNCL	Grouping class for collection privileges	DB2
GDSNDB	Grouping class for database privileges	DB2
GDSNPK	Grouping class for package privileges	DB2
GDSNPN	Grouping class for plan privileges	DB2
GDSNSG	Grouping class for storage group privileges	DB2
GDSNSM	Grouping class for system privileges	DB2
GDSNTB	Grouping class for table, index, or view privileges	DB2
GDSNTS	Grouping class for tablespace privileges	DB2
MDSNBP	Member class for buffer pool privileges	DB2
MDSNCL	Member class for collection privileges	DB2
MDSNDB	Member class for database privileges	DB2
MDSNPK	Member class for package privileges	DB2
MDSNPN	Member class for plan privileges	DB2
MDSNSG	Member class for storage group privileges	DB2
MDSNSM	Member class for system privileges	DB2
MDSNTB	Member class for table, index, or view privileges	DB2
MDSNTS	Member class for tablespace privileges	DB2
TMEADMIN	Maps the TME administrator's user ID and Tivoli Management Region (TMR) to a RACF user ID	TME 10

Commands

Figure 4 lists the changes to RACF commands for OS/390 Release 4.

For more information on these commands, see *OS/390 Security Server (RACF) Command Language Reference*.

Figure 4 (Page 1 of 3). Changes to RACF Commands

Command	Description	Support
ALTUSER PASSWORD	The ALTUSER command and the PASSWORD command are modified to save the old password in the password history list,whether reset by the user or an administrator. For more information on the ALTUSER and PASSWORD commands, see *OS/390 Security Server (RACF) Command Language Reference*.	Password History Enhancements

Figure 4 (Page 2 of 3). Changes to RACF Commands

Command	Description	Support
ALTUSER	This command supports the removal of all of the user's CLAUTH authorities by using NOCLAUTH(*). For more information on the ALTUSER NOCLAUTH keywords, see *OS/390 Security Server (RACF) Command Language Reference*.	TME 10
PERMIT	The PERMIT command allows the keywords WHEN(SYSID(*system-identifier* ...)). This specifies that the indicated users or groups have the specified access authority when loading this controlled program on the specified system. *system-identifier* is the 4-character value specified for the system identifier (SID) parameter of the SMFPRMxx member of PARMLIB. WHEN(SYSID(*system-identifier*)) can be used only for resources in the PROGRAM class. See *OS/390 MVS Initialization and Tuning Reference* for additional information on SMFPRMxx. For more information on the PERMIT command, see *OS/390 Security Server (RACF) Command Language Reference*.	Program control by SYSID

Figure 4 (Page 3 of 3). Changes to RACF Commands

Command	Description	Support
TARGET	The new keyword WDSQUAL is added to the RACF TARGET command to indicate that the variable that follows will be used by RRSF as the middle qualifier for the work space data set names of the INMSG and OUTMSG queues for the local RRSF node defined by the TARGET command. WDSQUAL cannot be used for a remote node. The format for the qualifier name is *prefix.wdsqual.ds_identity*. *wdsqual* can be from 1 to 8 characters long beginning with an alphabetic character. Initial numerals are not accepted. The formation of the workspace data set names can be changed until the data sets are allocated. This normally occurs when a DORMANT or OPERATIVE keyword is processed. After that keyword is processed, the data set names cannot be changed. Concerning TARGET nodename OPERATIVE WDSQUAL(xxx) , RACF processes the OPERATIVE keyword after the WDQUAL keyword, even though the user specified them in the reverse order. The keyword WDSQUAL works until RACF has processed a TARGET command specifying DORMANT or OPERATIVE for that node. This enhancement allows operators to set one or more work space data sets for local node names, which can be used when they are working with multisystem RRSF nodes, especially in a sysplex environment. If you have any TARGET commands in your IRROPTxx RACF parameter library member that specify the WORKSPACE keyword abbreviated to a W, you need to increase the length of that keyword to at least WO so it is not mistaken for the new WDSQUAL keyword which is now represented as W. If WDSQUAL is not specified, the previously used format for the data set names is used. This is *prefix.sysname*.INMSG and *prefix.sysname*.OUTMSG. For more information on the TARGET command, see *OS/390 Security Server (RACF) Command Language Reference*.	OW24966

Data Areas

Figure 5 lists changed product-sensitive programming interface (PSPI) data areas for RACF.

Figure 5. Changes to PSPI Data Areas

Data Area	Description	Support
AFC	This data area maps the contents for the Open Edition MVS security audit function codes. An audit function code has been added to audit when ck_priv is called from OpenEdition_spawn (BPX1SPN).	Auditability of super user requests.
COMP	This data area maps the common SAF/RACF parameter list for Open Edition MVS security functions. A new 24-byte DSECT ADMN has been added. It includes addresses of the function-specific parameter list structure, of the RACF user ID under whose authority the service executes, of a fullword containing the ACEE address under which this service executes, of a caller-supplied area containing the subpool in which output messages are obtained, and of a fullword containing a pointer to the RACF command output.	TME 10 GEM user administration for OS/390
FAST	FASTPLEN, FASTPVER, FASTALET, and FASTLOGS have been added.	DB2
FC	This data area maps the Open Edition MVS security function codes. A new constant IRRSEQ00# has been added for function code 39 - R_admin.	TME 10 GEM user administration for OS/390
RCVT	The RACF level in this data area has been updated to 2040, to reflect the new FMID, HRF2240.	New FMID
RFXP	RFXPLEN, RFXPVERS, RFXALET, and RFXLOGS have been added.	DB2
SAFP	This data area has been updated to reflect the new RACF FMID, HRF2240.	New FMID

Exits

Because two new keywords, ACEEALET and LOGSTR, were added to RACROUTE REQUEST=FASTAUTH, there are changes to exit processing.

When the ACEEALET keyword is specified on the RACROUTE REQUEST=FASTAUTH macro, the ACEE must be accessed using the ALET in the RFXALET field of the RFXP parameter list. In all other cases, the ACEE can be accessed in the current HOME address space. For cross-memory callers, this means the ACEE must be accessed using an ALET of 2.

When the ACEEALET= keyword is specified, the sequence of exit, authorization, and audit processing is the same as the sequence for cross-memory requests. This sequence is:

- ICHRFX03
- Authorization processing
- ICHRFX04
- Audit processing

RFXALET and RFXLOGS correspond to new fields in the RACROUTE REQUEST=FASTAUTH parameter list. These fields only exist in parameter lists created with RELEASE=2.4 or higher. Therefore, these fields must only be accessed when the RFXPVERS indicates Release 2.4 or higher.

Macros

Figure 6 lists changes to executable macros for OS/390 Release 4. These are for your information; there is no reason to modify any existing programs to specify the new release level. These changes are general-use programming interfaces (GUPI).

Figure 6. Changed Executable Macros

Macro	Description	Support
ICHEACTN ICHEINTY ICHETEST	These macros accept the new RELEASE=2.4 keyword.	New FMID
RACROUTE	REQUEST=FASTAUTH allows the following to be specified: • LOGSTR=*parameter* • Message suppression (MSGSUPP=YES) • ACEEALET=*alet_addr parameter*	Authorization support for DB2

Messages

The messages that have been added or changed in RACF for OS/390 Release 4 are listed below. Compare the message identifiers and the corresponding message text with any automated operations procedures your installation uses to determine whether updates are required.

New Messages

The following messages are added:

PERMIT Command Messages ICH06021I

RACF/DB2 External Security Module Messages: IRR900A, IRR901A, IRR902A, IRR903A, IRR904I, IRR905I, IRR906I, IRR907I, IRR908I, IRR909I, IRR910I, IRR911I

TARGET Command Messages: IRRM055I, IRRM056I

Changed Messages

The following messages are changed:

RACF Initialization Messages: ICH502I, ICH506I, ICH518I, ICH556I

PERMIT Command Messages: ICH06018I

RDEFINE Command Messages: ICH10302I

RALTER Command Messages: ICH11304I

SETROPTS Command Messages: ICH14042I

RACF Manager Error Messages: ICH51011I

RACF Processing Messages: IRR410I

RACF Utility Messages: IRR67032I, IRR67034I, IRR67124I, IRR67153I, IRR67183I

RRSF Enveloping Messages: IRRV002I, IRRV005I, IRRV013I, IRRV014I

RACF Operational Modes and Coupling Facility Messages: IRRX013A

Deleted Messages

The following messages have been deleted:

ICH401I, ICH402I, ICH403I, ICH404I, ICH405I, ICH406I, ICH407I, ICH410I, ICH413I, ICH536I, ICH543I, ICH547I, ICH548I, ICH61000I, ICH61001I, ICH61002I, ICH61003I, ICH61004I, ICH61006I, ICH61007I, ICH62001I, ICH62002I, ICH62003I, ICH62004I, ICH62007I, ICH62008I, ICH62009I, ICH62010I, ICH62012I, ICH62014I, ICH62015I, ICH62017I, ICH62018I, ICH62019I, ICH62021I, ICH62022I, ICH63001I, ICH63002I, ICH63003I, ICH63004I, ICH63005I, ICH63006I, ICH63007I, ICH63008I, ICH63009I, ICH63010I, ICH63011I, ICH63012I, ICH63013I, ICH63014I, ICH63015I, ICH63016I, ICH63017I, ICH63018I, ICH63019I, ICH63020I, ICH63021I, ICH63022I, ICH63023I, ICH63024I, ICH63025I, ICH63026I, ICH63027A, ICH65001I, ICH65002I, ICH65003I, ICH65004I, ICH65005I, ICH65006I, ICH65007I, ICH65008I, ICH65009I, ICH65010I, ICH65011I, ICH65012I, ICH65013I, ICH65014I, ICH65015I, ICH65016I, ICH65017I, ICH65018I, ICH65019I, ICH65020I, ICH65021I, ICH65022I, ICH65023I, ICH65024I, ICH65025I, ICH65026I, ICH8000, ICH8001, ICH8002, ICH8003, ICH8004, ICH8005, ICH8006, ICH8007, ICH8008, ICH8009, ICH8010, ICH8011, ICH8012, ICH8013, ICH8014, ICH8015, ICH8016, ICH10316I, ICH36001I, IRR67098I

Panels

Figure 7 lists new RACF panels. Figure 8 on page 19 lists RACF panels that are changed.

Figure 7. New Panels for RACF

Panel	Description	Support
ICHP241n	This panel enables you to add an entry for the conditional access list and to identify the access authority for it.	Program control by system ID
ICHP242n	This panel enables you to remove an entry from the conditional access list and to identify the access list from which conditions are to be removed	Program control by system ID
ICHH241n	This panel allows you to specify the system identifiers (SMFIDs) of the systems from which users may use the resources protected by the profile. Each system identifier is a 4-characters string.	Program control by system ID
ICHH242n	This panel allows you to specify the system identifiers (SMFIDs) of the systems to be removed from the specified entries in the conditional access list. Each system identifier is a 4-character string.	Program control by system ID
ICHnnnn	This panel enables you to specify identifiers (SMFIDs) of the system from which users may use the resources that are being protected. Each system identifier is a 4-character string.	Program control by system ID
ICHHnnnn	This panel enables you to specify identifiers (SMFIDs) of the system to be removed from the specified entries in the conditional access list. Each system identifier is a 4-character string.	Program control by system ID

Figure 8. Changed Panels for RACF

Panel	Description	Support
ICHP241C ICHP242A ICHH241C	These panels contain changes needed to add or remove list entries related to conditional access lists.	Program control by system ID

SYS1.SAMPLIB

Figure 9 identifies change to the RACF member of SYS1.SAMPLIB.

Figure 9. Change to SYS1.SAMPLIB

Member	Description	Support
IRR@XACS	This member is shipped to provide a sample RACF authorization check external security module.	Authorization support for DB2

Publications Library

Figure 10 lists changes to the OS/390 Security Server (RACF) publications library.

Figure 10. Changes to the RACF Publications Library

Publication	Change
OS/390 Security Server (RACF) Callable Services	This publication is available only in softcopy.
OS/390 Security Server (RACF) Data Areas	This is no longer a licensed publication. Its new form number is SY27-2640-03.

Note:

You are able to print the softcopy documentation, either in its entirety or simply portions of it.

Chapter 4. Planning Considerations

This chapter describes the following high-level planning considerations for customers upgrading to OS/390 Release 4 Security Server (RACF) from OS/390 Release 3 Security Server (RACF):

- Migration strategy
- Migration paths
- Hardware requirements
- Compatibility

Migration Strategy

The recommended steps for migrating to a new release of RACF are:

1. Become familiar with the release documentation.
2. Develop a migration plan for your installation.
3. Install the product using the program directory shipped with OS/390.
4. Use the new release before initializing major new function.
5. Customize the new function for your installation.
6. Exercise the new function.

Migration Paths for OS/390 Release 4 Security Server (RACF)

- From OS/390 Release 3 Security Server (RACF)

  If you are an OS/390 Release 3 Security Server (RACF) customer, you can migrate to OS/390 Release 4 Security Server (RACF) if you meet the OS/390 release requirements.

- From OS/390 Release 2 Security Server (RACF)

  If you are an OS/390 Release 2 Security Server (RACF) customer, you can migrate to OS/390 Release 4 Security Server (RACF) if you meet the OS/390 release requirements. You should also read *OS/390 Security Server (RACF Planning: Installation and Migration* for Release 3.

- From OS/390 Release 1 Security Server (RACF) or RACF 2.2

  If you are an OS/390 Release 1 Security Server (RACF) or RACF 2.2 customer, you can migrate to OS/390 Release 4 Security Server (RACF) if you meet the OS/390 release requirements. (OS/390 Release 1 Security Server (RACF) and RACF 2.2 are functionally equivalent.) In addition to this book, you should read:

  – *OS/390 Security Server (RACF) Planning: Installation and Migration* for OS/390 Release 2 (GC28-1920-01) and Release 3 (GC28-1920-02)

- From RACF 1.9.2 or RACF 2.1

  If you are a RACF 1.9.2 or 2.1 customer, you can migrate to OS/390 Release 4 Security Server (RACF) if you meet the OS/390 release requirements. If you have RACF 2.1 installed, in addition to this book, you should read:

  – *OS/390 Security Server (RACF) Planning: Installation and Migration* for OS/390 Release 2 (GC28-1920-01) and Release 3 (GC28-1920-02), and

© Copyright IBM Corp. 1994, 1997

– *OS/390 Security Server (RACF) Planning: Installation and Migration* for OS/390 Release 1.(GC28-1920-00)

If you have RACF 1.9.2 installed, in addition to this book, you should read:

– *OS/390 Security Server (RACF) Planning: Installation and Migration* for OS/390 Release 2, (GC28-1920-01) and Release 3 (GC28-1920-02)

– *OS/390 Security Server (RACF) Planning: Installation and Migration* for OS/390 Release 1(GC28-1920-00)

– *RACF Planning: Installation and Migration* for RACF 2.1 (GT00-9241-00)

- From RACF 1.9

  If you are a RACF 1.9 customer, you can migrate to OS/390 Release 4 Security Server (RACF) if you are running with the restructured database and meet the OS/390 release requirements. If your database is not restructured, you must restructure it and perform appropriate testing of any installation-supplied code that uses ICHEINTY or RACROUTE REQUEST=EXTRACT,TYPE=EXTRACT or TYPE=REPLACE before installing OS/390 Release 2 Security Server (RACF). In addition to this book, you should read:

  – *OS/390 Security Server (RACF) Planning: Installation and Migration* for OS/390 Release 2 (GC28-1920-01) and Release 3 (GC28-1920-02)

  – *OS/390 Security Server (RACF) Planning: Installation and Migration* for OS/390 Release 1 (GC28-1920-00)

  – *RACF Migration and Planning* for RACF 2.1(GT00-9241-00)

  – *RACF Migration and Planning* for RACF 1.9.2(GC23-3045)

  From RACF releases prior to 1.9

  If you are on a RACF release prior to 1.9, you need to buy a conversion service. These are available from IBM and possibly from other vendors. In addition to this book, you should read:

  – *OS/390 Security Server (RACF) Planning: Installation and Migration* for OS/390 Release 2 (GC28-1920-01) and Release 3 (GC28-1920-02)

  – *OS/390 Security Server (RACF) Planning: Installation and Migration* for OS/390 Release 1 (GC28-1910-00)

  – *RACF Planning: Installation and Migration* for RACF 2.1 (GT00-9241-00)

  – *RACF Migration and Planning* for RACF 1.9.2 (GC23-3054)

  – *RACF Migration and Planning* for RACF 1.9 (GT00-5380-00)

Hardware Requirements

OS/390 Release 4 Security Server (RACF) does not require any specific hardware support. It runs on all hardware supported by OS/390 Release 4. However, data sharing mode in the Parallel Sysplex requires a coupling facility configured for RACF's use.

Compatibility

This section describes considerations for compatibility between OS/390 Release 4 Security Server (RACF) and OS/390 Release 3 Security Server (RACF).

OpenEdition MVS

If you are an OpenEdition MVS user, be sure to review carefully the following information on possible changes.

For Auditability of Superusers

If you are not already auditing the PROCESS class, you need to decide whether you want to receive the audit records. If you do decide you wish to audit the OpenEdition spawn service, issue SETROPTS LOGOPTIONS(xxxx(PROCESS)) to obtain the SMF TYPE80 record ck_priv in order to audit superuser use. If you are auditing the PROCESS class, you do not need to issue that command.

You need to change any programs reporting from the unloaded data if you want the spawn audit information.

For Default USER/GROUP OpenEdition Segment

The existing type 317 relocate section appears on any SMF TYPE80 records written by the RACF callable services for users running with any default OpenEdition information.

You need to change any programs reporting from the unloaded data if you use this support.

Program Control by System ID

If users are already allowed access through the standard access list, they must be removed from these lists so the conditional access list entry is used. In-storage program profiles must be refreshed with SETROPTS WHEN(PROGRAM) REFRESH to activate the updated PROGRAM profiles.

RELEASE=2.4 Keyword on Macros

You should only specify RELEASE=2.4 and reassemble if you intend to use the new keywords. If you use the new keywords, you need to run the program on an OS/390 Release 4 system to get the expected results.

Chapter 5. Installation Considerations

This chapter describes the following changes of interest to the system programmer installing OS/390 Release 4 Security Server (RACF):

- Virtual storage considerations
- Templates

RACF Storage Considerations

This section discusses storage considerations for RACF.

Using the RACF DB2 external security module increases the number of profiles in the RACF database. Therefore, if you plan to use the RACF DB2 external security module, recalculate the amount of storage that is needed. If there is not enough storage, you should increase the size of the RACF database.

Virtual Storage

Figure 11 estimates RACF virtual storage usage for planning purposes.

Figure 11 (Page 1 of 3). RACF Estimated Storage Usage

Storage Subpool	Usage	How to Estimate Size
FLPA	RACF service routines, if IMS or CICS is using RACF for authorization checking	47 000
	RACROUTE REQUEST=FASTAUTH and ICHRTX00 exits	Measure using AMBLIST
PLPA	RACF installation exits that are AMODE(24) or AMODE(ANY)	Measure using AMBLIST
	RACF RMODE(24) code	750
	RACF service routines, if IMS or CICS is not using RACF for authorization checking, unless explicitly removed from SYS1.LPALIB and placed elsewhere for use in FLPA	47 000
	RACROUTE REQUEST=FASTAUTH and ICHRTX00 exits	Measure using AMBLIST
	RACF range table	4 + (number_of_ranges × 45)
EPLPA	RACF installation exits that are AMODE(31)	Measure using AMBLIST
	RACF resident modules above 16MB	875 000
SQA	RACF communications vector table and extension	2800
	Class descriptor table (CNST) and RACF router table	7500 + 58 × number_of_customer_defined_classes

© Copyright IBM Corp. 1994, 1997

Figure 11 (Page 2 of 3). RACF Estimated Storage Usage

Storage Subpool	Usage	How to Estimate Size
ESQA	RACF data sharing control area	300 (when enabled for sysplex communication)
	Class descriptor table (CNSX)	(number_of_IBM-defined_classes × 28) + (number_of_IBM-defined_entries_in_router_table × 30) + (number_of_customer_defined_classes × 58) + 26 For Security Server (RACF), there are 145 IBM-defined classes and 167 IBM-defined entries in the router table, so the size of the CNSX is 9096 + (number_of_customer_defined_classes × 58). If you install a PTF that adds entries, you will need to recalculate this number.
LSQA	ACEE and related storage **Notes:** 1. Applications can place this storage in a different subpool. 2. Applications can create multiple ACEEs in this and other storage subpools.	400 + installation_data_length + terminal_installation_data_length + application_installation_data + (52 for every 78 temporary datasets, rounded up to the next multiple of 52) If the address space has been dubbed an OpenEdition process, then add: 52 + (number_of_connected_groups_with_GIDs × 4) Add 112 bytes if the user has CLAUTH for a class with a POSIT value over 127.
ELSQA	Connect group table	64 + (48 × number_of_groups_connected)
	In-storage generic profiles	160 + number_of_generic_profiles × (14 + average_profile_size + average_profile_name_length)
	RACF storage tracking table	3500
	RACROUTE REQUEST=LIST profiles **Note:** Applications can place these profiles in a different storage subpool.	2108 + (number_of_profiles_in_class × 16) + (number_of_unique_generic_profile_prefix_lengths × 24) + (number_of_generic_profiles × 4) + (number_of_resident_profiles × (10 + average_profile_size + (1.5 × class_max_profile_name_size))) for each class if GLOBAL=YES is not specified
CSA	RACF global access tables	3040 + (number_of_user_classes × 24) + 2 × (18 + number_of_entries × (6 + (1.5 × max_profile_name_size)))
	RACF database control structures (DCB, DEB, templates)	4600 + (number_of_BAM_blocks × 6) + (364 x number_of_RACF_primary_data_sets)
	RACF subsystem control blocks	3500

Figure 11 (Page 3 of 3). RACF Estimated Storage Usage

Storage Subpool	Usage	How to Estimate Size
ECSA	RACF data set descriptor table and extension	168 + (896 × number_of_RACF_primary_data_sets)
	RACF ICB (non-shared DB)	4096 per RACF database if the database is not shared and is not on a device marked as shared, 0 otherwise
	RACF program control table	28 + (number_of_program_profiles × average_program_profile_size) + (number_of_controlled_libraries × 50) To find the average_program_profile_size, use the following formula: 54 + (average_number_of_access _entries × 9) + (average_number_of _conditional_access_entries × 17) + (average_number_of_libraries × 52)
	RACF resident data blocks	For each primary RACF database: 3248 + (4136 × number_of_database_buffers) If using sysplex communication, for each backup database add: 3248 + (4136 × number_of_database_buffers × 2)
	Dynamic parse tables	30 000
	SETROPTS GENLIST profiles	52 + (number_of_profiles_in_class × 16) + (number_of_resident_profiles × (10 + average_profile_size + (1.5 × class_max_profile_name_size)))
User private Below 16MB	RACF transient storage	16 000 (minimum) while a RACF service is executing

Templates for RACF on OS/390 Release 4

The RACF database must have templates at the Security Server (RACF) Release 4 level in order for RACF to function properly. If a Security Server (RACF) Release 4 system is sharing the database with a lower-level system (RACF 1.9, RACF 1.9.2, RACF 1.10, RACF 2.1, RACF 2.2, Security Server (RACF) Release 1, Security Server (RACF) Release 2, or Security Server (RACF) Release 3), the lower-level system is able to use the database with the Security Server (RACF) Release 4 templates. Use the IRRMIN00 utility to install the templates.

For more information, see *OS/390 Security Server (RACF) System Programmer's Guide* and the program directory shipped with OS/390.

Chapter 6. Customization Considerations

This chapter identifies customization considerations for OS/390 Release 4 Security Server (RACF).

For additional information, see *OS/390 Security Server (RACF) System Programmer's Guide*.

Customer Additions to the Router Table and the CDT

Installations must verify that classes they have added to the router table and class descriptor table (CDT) do not conflict with new classes shipped with RACF. If duplicate table entries are detected, the following error messages are issued at IPL time:

- For a duplicate router table entry, RACF issues this message and continues processing: `ICH527I RACF DETECTED AN ERROR IN THE INSTALLATION ROUTER TABLE, ENTRY class_name, ERROR CODE 1.`
- For a duplicate CDT entry, RACF issues this message and enters failsoft mode: `ICH564A RACF DETECTED AN ERROR IN THE INSTALLATION CLASS DESCRIPTOR TABLE, ENTRY class_name, ERROR CODE 7.`

If a conflict in class names occurs, you must delete the profiles in the installation-defined class with the conflicting name, delete the CDT entry for the class, add a CDT entry with a different name, and redefine the profiles.

Do not assemble the user-defined CDT (ICHRRCDE) on OS/390 Release 4 and attempt to use it on a system running RACF at a lower level than RACF Version 2 Release 2.

RACF/DB2 External Security Module Customization

If you have both this release of RACF and Version 5 of DB2, you can use RACF to protect DB2 objects. Migrating to this can be done one object at a time. For example, all DB2 tables can be protected by RACF while other DB2 objects are not RACF-protected. If an object is not protected by RACF, the RACF/DB2 external security module defers to DB2 for authority checking.

The following is an overview of the steps involved in customizing RACF/DB2 external security module. For details, see *OS/390 Security Server (RACF) System Programmer's Guide* and *OS/390 Security Server (RACF) Security Administrator's Guide*

- Concerned staff members, such as the security administrator, system programmer, DB2 system programmer, and database administrator, need to decide whether to use the RACF/DB2 external security module.
- Staff members need to decide which of the options (such as class and profile name options) offered by the RACF/DB2 external security module they plan to use. This can be as simple as using the defaults, which is recommended. If the defaults are used, no new classes are needed.

© Copyright IBM Corp. 1994, 1997

- Set the options in the RACF/DB2 external security module. To do this, see *OS/390 Security Server (RACF) System Programmer's Guide*.
- Decide which DB2 objects are to be protected using RACF. Define the appropriate profiles. To do this, see *OS/390 Security Server (RACF) Security Administrator's Guide*.
- Activate the RACF/DB2 external security module. This includes assembling and linkediting the RACF/DB2 external security module. In addition confirm that it is in the appropriate library. To do this, see *DB2 for OS/390 Version 5 Administration Guide Volume 2*, SC26-8957, and *DB2 for OS/390 Version 5 Installation Guide*, GC26-8970.
- Restart the DB2 subsystem.

Exit Processing

The following changes affect FASTAUTH exits. Four fields have been added to the RFXP data area and four to the FAST data area.

Four fields are added to the RFXP data area. These are two 1-byte fields, RFXPLEN and RFXPVERS. RFXPLEN contains the parameter list length, and RFXPVERS contains the parameter list version. There are also two new 4-byte fields, RFXALET and RFXLOGS, which exist only when RFXPVERS contains a value of 1 or higher.

Four fields are also added to the FAST data area. These are two 1-byte fields, FASTPLEN and FASTPVER. FASTPLEN contains the parameter list length, and FASTPVER contains the parameter list version. There are also two new 4-byte fields, FASTALET and FASTLOGS, which exist only when FASTPVER contains a value of 1 or higher.

Chapter 7. Administration Considerations

This chapter summarizes the changes to administration procedures that the security administrator should be aware of. For more information, see *OS/390 Security Server (RACF) Security Administrator's Guide*.

The TMEADMIN Class

The new TMEADMIN class is used to associate a TME administrator with a RACF MVS identity on any MVS system that is part of a Tivoli management region (TMR). The TMEADMIN class contains a profile for each TME administrator who is able to perform RACF user management tasks. The name of this profile is the TME administrator string name. For example:

```
admin-login-name@TME-region-name
```

The hex code for @ is x'7C'. You need to use the key on your keyboard that provides that hex value. Sharing of a single RACF user ID by multiple TME administrators is not recommended. It is preferable that each TME administrator ID map to a unique RACF user ID.

In the following example, the TME administrator root in the Tivoli TMR region of pok01 would have a RACF user ID of CSMITH. The APPLDATA field of this profile contains the RACF MVS userid. Only a RACF administrator with SPECIAL authority can issue this command:

```
RDEFINE  TMEADMIN root@pok01 APPLDATA('CSMITH')
```

For more information on the TMEADMIN class, see “Tivoli Management Environment (TME) 10 Global Enterprise Management User Administration Service” on page 8.

Password History Changes

When an administrator resets a password for a user, the old password is saved in the password history list. This is done with the use of one of the following commands:

```
ALTUSER (userid ...) PASSWORD
ALTUSER (userid ...) PASSWORD(password)
PASSWORD USER(userid ...)
```

For more information, see “Password History Enhancements” on page 7.

Program Control by System ID

Program control by system ID limits a user's access to a particular program to a specified system. It improves system management and usability of program products in the sysplex environment. In addition, it eliminates error-prone manual procedures, eliminates the need to keep DASD that is not shared, and eliminates the possibility of license exposures.

© Copyright IBM Corp. 1994, 1997

Enhancements of Global Access Checking

When you use RACROUTE REQUEST=AUTH processing (which utilizes global access checking) for general resource classes, these classes can be processed whether or not the class is RACLISTed using SETROPTS RACLIST or RACROUTE REQUEST=LIST.

Chapter 8. Auditing Considerations

This section summarizes the changes to auditing procedures for SMF records.

SMF Records

Figure 12 summarizes changes to SMF records created by RACF for OS/390 Release 4. These changes are general-use programming interfaces (GUPI).

Figure 12. Changes to SMF Records

Record Type	Record Field	Description of Change	Support
80	SMF80DTA	When program control through system ID is operating, a new bit is defined in an existing relocate section for SMF TYPE80 records written by the PERMIT command. The relocate section is data type 39 (X'27'), and the new bit indicates that the conditional entity type is SYSID.	Program control through system ID
80	SMF80DA2	This record with a ck_priv event code is written when an authorization check is done for a superuser. The record contains the audit function code to indicate that the ck_priv callable service was called from spawn (IRRSPK00).	OpenEdition auditing of superuser use

For more information on SMF records, see *OS/390 Security Server (RACF) Macros and Interfaces*.

The RACF/DB2 external security module can be used to protect DB2 objects using RACF profiles. If your installation chooses to use this function, RACF SMF Type 80 records can be used to audit access attempts to DB2 data and resources. For more information on auditing for the RACF/DB2 external security module, see *OS/390 Security Server (RACF) Auditor's Guide*.

© Copyright IBM Corp. 1994, 1997

Chapter 9. Application Development Considerations

Application development is the process of planning, designing, and coding application programs that invoke RACF functions. This section highlights new support that might affect application development procedures:

- Programming interfaces
- RELEASE=2.4 keyword on macros
- Changes to RACROUTE REQUEST=FASTAUTH

Programming Interfaces

For a summary of changes to the programming interfaces for RACF for OS/390 Release 4, see:

- "Class Descriptor Table (CDT)" on page 12
- "Data Areas" on page 15
- Figure 6 on page 17

RELEASE=2.4 Keyword on Macros

The RACROUTE, ICHEINTY, ICHEACTN, and ICHETEST macros support the value 2.4 on the RELEASE keyword, although they do not support new keywords that would require RELEASE=2.4 to be specified. Customers are not required to update existing programs to specify RELEASE=2.4. You should only use the RELEASE=2.4 keyword if you are using new keywords.

FASTAUTH Changes

Changes in this release allow:

- LOGSTR= parameter to be specified on the RACROUTE REQUEST=FASTAUTH macro
- Message suppression (MSGSUPP=YES) to be specified on the RACROUTE REQUEST=FASTAUTH macro
- ACEEALET=alet_addr parameter on RACROUTE REQUEST=FASTAUTH to specify ALET value of any address space where an ACEE resides

© Copyright IBM Corp. 1994, 1997

Chapter 10. General User Considerations

RACF general users use RACF to:

- Log on to the system
- Access resources on the system
- Protect their own resources and any group resources to which they have administrative authority

For more information on the output general users might receive, see *OS/390 Security Server (RACF) General User's Guide*.

Password History Changes

End users are no longer able to keep their favorite password by pretending they have forgotten it and getting a security administrator or help desk person to reset it to a temporary value for them. RACF saves the old (favorite) password in the history list, making it unusable.

© Copyright IBM Corp. 1994, 1997

Glossary

A

access. The ability to obtain the use of a protected resource.

access authority. An authority related to a request for a type of access to protected resources. In RACF, the access authorities are NONE, EXECUTE, READ, UPDATE, CONTROL, and ALTER.

accessor environment element (ACEE). A description of the current user, including user ID, current connect group, user attributes, and group authorities. An ACEE is constructed during user identification and verification.

ACEE. See *accessor environment element*.

appropriate privileges. In the OpenEdition MVS implementation, superuser authority. A trusted or privileged attribute is an attribute associated with a started procedure address space and with any process associated with the address space.

AUDIT request. The issuing of the RACROUTE macro with REQUEST=AUDIT specified. An AUDIT request is a general-purpose security-audit request that can be used to audit a specified resource name and action.

AUTH request. The issuing of the RACROUTE macro with REQUEST=AUTH specified. The primary function of an AUTH request is to check a user's authorization to a RACF-protected resource or function. The AUTH request replaces the RACHECK function. See also *authorization checking*.

authority. The right to access objects, resources, or functions. See *access authority, class authority,* and *group authority*.

authorization checking. The action of determining whether a user is permitted access to a protected resource. RACF performs authorization checking as a result of a RACROUTE REQUEST=AUTH or RACROUTE REQUEST=FASTAUTH.

automatic command direction. An extension of command direction that causes RACF to automatically direct certain commands to one or more remote nodes after running the commands on the issuing node. Commands can be automatically directed based on who issued the command, the command name, or the profile class related to the command. Profiles in the RRSFDATA class control to which nodes commands are automatically directed. See also *automatic password direction*, *automatic command direction*, *automatic direction of application updates*, and *command direction*.

automatic direction. An RRSF function that automatically directs commands, ICHEINTY and RACROUTE macros, and password-related updates to one or more remote systems. See also *automatic command direction*, *automatic password direction*, and *automatic direction of application updates*.

automatic direction of application updates. An RRSF function that automatically directs ICHEINTY and RACROUTE macros that update the RACF database to one or more remote systems. Profiles in the RRSFDATA class control which macros are automatically directed, and to which nodes. See also *automatic direction*, *automatic command direction*, and *automatic password direction*.

automatic password direction. An extension of password synchronization and automatic command direction that causes RACF to automatically change the password for a user ID on one or more remote nodes after the password for that user ID is changed on the local node. Profiles in the RRSFDATA class control for which users and nodes passwords are automatically directed. See also *password synchronization, automatic command direction, automatic direction of application updates, and automatic direction.*

C

cache structure. A coupling facility structure that contains data accessed by systems in a sysplex. MVS provides a way for multiple systems to determine the validity of copies of the cache structure data in their local storage.

callable service. In OpenEdition MVS, a request by an active process for a service. Synonymous with *syscall*, *system call*.

CDT. See *class descriptor table*.

class. A collection of RACF-defined entities (users, groups, and resources) with similar characteristics. The class names are USER, GROUP, DATASET, and the classes that are defined in the class descriptor table.

class authority (CLAUTH). An authority enabling a user to define RACF profiles in a class defined in the class descriptor table. A user can have class authorities to one or more classes.

class descriptor table (CDT). A table consisting of an entry for each class except the USER, GROUP, and

© Copyright IBM Corp. 1994, 1997

DATASET classes. The table is generated by executing the ICHERCDE macro once for each class. The class descriptor table contains both the IBM provided classes and also the installation defined classes.

CLAUTH. See *class authority*.

command direction. A RRSF function that allows a user to issue a command from one user ID and direct that command to run under the authority of a different user ID on the same or a different RRSF node. Before a command can be directed from one user ID to another, a user ID association must be defined between them via the RACLINK command.

command interpreter. A program that reads the commands that you type in and then executes them. When you are typing commands into the computer, you are actually typing input to the command interpreter. The interpreter then decides how to perform the commands that you have typed. The shell is an example of a command interpreter. Synonymous with *command language interpreter*. See also *shell*.

command language interpreter. Synonym for *command interpreter*.

coupling facility. The hardware element that provides high-speed caching, list processing, and locking functions in a sysplex.

D

Data Facility Product (DFP). A program that isolates applications from storage devices, storage management, and storage device hierarchy management.

data security. The protection of data from unauthorized disclosure, modification, or destruction, whether accidental or intentional.

data security monitor (DSMON). A RACF auditing tool that produces reports enabling an installation to verify its basic system integrity and data-security controls.

data set profile. A profile that provides RACF protection for one or more data sets. The information in the profile can include the data-set profile name, profile owner, universal access authority, access list, and other data. See *discrete profile* and *generic profile*.

data sharing mode. An operational RACF mode that is available when RACF is enabled for sysplex communication. Data sharing mode uses global resource serialization protocol that allows concurrent RACF instances to directly access and change the same database while maintaining data integrity as always. Data sharing mode requires installation of coupling facility hardware.

default group. In RACF, the group specified in a user profile that is the default current connect group.

DEFINE request. The issuing of the RACROUTE macro with REQUEST=DEFINE specified. Also, using a RACF command to add or delete a resource profile causes a DEFINE request. The DEFINE request replaces the RACDEF function.

DFP. See Data Facility Product.

DFP segment. The portion of a RACF profile containing information relating to the users and resources that are managed by the data facility product (DFP).

DIRAUTH request. The issuing of the RACROUTE macro with REQUEST=DIRAUTH specified. A DIRAUTH request works on behalf of the message-transmission managers to ensure that the receiver of a message meets security-label authorization requirements.

directed command. A RACF command that is issued from a user ID on an RRSF node. It runs in the RACF subsystem address space on the same or a different RRSF node under the authority of the same or a different user ID. A directed command is one that specifies AT or ONLYAT. See also *command direction* and *automatic command direction*.

directory. (1) A type of file containing the names and controlling information for other files or other directories. (2) A construct for organizing computer files. As files are analogous to folders that hold information, a directory is analogous to a drawer that can hold a number of folders. Directories can also contain subdirectories, which can contain subdirectories of their own. (3) A file that contains directory entries. No two directory entries in the same directory can have the same name. (4) A file that points to files and to other directories. (5) An index used by a control program to locate blocks of data that are stored in separate areas of a data set in direct access storage.

discrete profile. A resource profile that can provide RACF protection for only a single resource. For example, a discrete profile can protect only a single data set or minidisk.

DSMON. See *data security monitor*.

E

entity. A user, group, or resource (for example, a DASD data set) that is defined to RACF.

EXTRACT request. The issuing of the RACROUTE macro with REQUEST=EXTRACT specified. An EXTRACT request retrieves or replaces certain specified fields from a RACF profile or encodes certain clear-text (readable) data. The EXTRACT request replaces the RACXTRT function.

F

FASTAUTH request. The issuing of the RACROUTE macro with REQUEST=FASTAUTH specified. The primary function of a FASTAUTH request is to check a user's authorization to a RACF-protected resource or function. A FASTAUTH request uses only in-storage profiles for faster performance. The FASTAUTH request replaces the FRACHECK function. See also *authorization checking*.

G

general resource. Any system resource, other than an MVS data set, that is defined in the class descriptor table (CDT). General resources are DASD volumes, tape volumes, load modules, terminals, IMS and CICS transactions, and installation-defined resource classes.

general resource profile. A profile that provides RACF protection for one or more general resources. The information in the profile can include the general resource profile name, profile owner, universal access authority, access list, and other data.

general-use programming interface (GUPI). An interface that IBM makes available for use in customer-written programs with few restrictions and that does not require knowledge of the detailed design or implementation of the IBM software product. See also *product-sensitive programming interface (PSPI)*.

generic profile. A resource profile that can provide RACF protection for one or more resources. The resources protected by a generic profile have similar names and identical security requirements. For example, a generic data-set profile can protect one or more data sets.

GID. See *group identifier*.

group. A collection of RACF-defined users who can share access authorities for protected resources.

group authority. An authority specifying which functions a user can perform in a group. The group authorities are USE, CREATE, CONNECT, and JOIN.

group identifier (GID). (1) In OpenEdition MVS, a unique number assigned to a group of related users. The GID can often be substituted in commands that take a group name as an argument. (2) A non-negative integer, which can be contained in an object of type *gid_t,* that is used to identify a group of system users. Each system user is a member of at least one group. When the identity of a group is associated with a process, a group ID value is referred to as a real group ID, an effective group ID, one of the (optional) supplementary group IDs, or an (optional) saved set-group-ID.

group profile. A profile that defines a group. The information in the profile includes the group name, profile owner, and users in the group.

GUPI. See *general-use programming interface*.

H

HFS. See *hierarchical file system*.

hierarchical file system (HFS). Information is organized in a tree-like structure of directories. Each directory can contain files or other directories.

I

ICB. See *inventory control block*.

inventory control block (ICB). The first block in a RACF database. The ICB contains a general description of the database.

K

kernel. (1) In OpenEdition MVS, the part of an operating system that contains programs for such tasks as I/O, management, and control of hardware and the scheduling of user tasks. (2) The part of the system that is an interface with the hardware and provides services for other system layers such as system calls, file system support, and device drivers. (3) The part of an operating system that performs basic functions such as allocating hardware resources. (4) A program that can run under different operating system environments. See also *shell*. (5) A part of a program that must be in central storage in order to load other parts of the program.

L

LIST request. The issuing of the RACROUTE macro with REQUEST=LIST specified. A LIST request builds in-storage profiles for RACF-defined resources. The LIST request replaces the RACLIST function.

local logical unit (LU). Local LUs are LUs defined to the MVS system; partner LUs are defined to remote systems. It is a matter of point of view. From the point of view of a remote system, LUs defined to that system are local LUs, and those on MVS are the partner LUs.

A partner LU might or might not be on the same system as the local LU. When both LUs are on the same system, the LU through which communication is initiated is the local LU, and the LU through which communication is received is the partner LU.

local node. The RRSF node from whose point of view you are talking. For example, if MVSA and MVSB are two RRSF nodes that are logically connected, from MVSA's point of view MVSA is the local node, and from MVSB's point of view MVSB is the local node. See also *remote node*.

logical unit. A port providing formatting, state synchronization, and other high-level services through which an end user communicates with another end user over an SNA network.

LU. See *logical unit*.

M

main system. The system on a multisystem RRSF node that is designated to receive most of the RRSF communications sent to the node.

member system. Any one of the MVS system images in a multisystem RRSF node.

multisystem node. See *multisystem RRSF node*

multisystem RRSF node. An RRSF node consisting of multiple MVS system images that share the same RACF database. One of the systems is designated to be the main system, and it receives most of the RRSF communications sent to the node.

MVS. Multiple virtual storage. Implies MVS/370, MVS/XA, and MVS/ESA.

N

NetView segment. The portion of a RACF profile containing NetView logon information.

node. See RRSF node.

O

OVM segment. The portion of a RACF profile containing OVM logon information.

owner. The user or group who creates a profile or is named the owner of a profile. The owner can modify, list, or delete the profile.

P

partner logical unit (partner LU). Partner LUs are LUs defined to remote systems; LUs defined to the MVS system are local LUs. It is a matter of a point of view. From the point of view of the remote system, LUs defined to that system are local LUs, and the ones on MVS are the partner LUs.

A partner LU might or might not be on the same system as the local LU. When both LUs are on the same system, the LU through which communication is initiated is the local LU, and the LU through which communication is received is the partner LU.

PassTicket. An alternative to the RACF password that permits workstations and client machines to communicate with the host. It allows a user to gain access to the host system without sending the RACF password across the network.

password. In computer security, a string of characters known to the computer system and a user who must specify it to gain full or limited access to a system and to the data stored within it. In RACF, the password is used to verify the identity of the user.

password synchronization. An option which can be specified when a peer user ID association is defined between two user IDs. If password synchronization is specified for a user ID association, then whenever the password for one of the associated user IDs is changed, the password for the other user ID is automatically changed to the newly defined password. See also *automatic password direction*.

permission bits. In OpenEdition MVS, part of security controls for directories and files stored in the hierarchical file system (HFS). Used to grant read, write, search (just directory), or execute (just file) access to owner, owner's group, or all others.

posit. A number specified for each class in the class descriptor table that identifies a set of flags that control RACF processing options. See the keyword description for posit in *OS/390 Security Server (RACF) Macros and Interfaces*.

process. (1) A function being performed or waiting to be performed. (2) An executing function, or one waiting to execute. (3) A function, created by a **fork()** request, with three logical sections:

- Text, which is the function's instructions
- Data, which the instructions use but do not change
- Stack, which is a push-down, pop-up save area of the dynamic data that the function operates upon

The three types of processes are:

- User processes, which are associated with a user at a workstation
- Daemon processes, which do systemwide functions in user mode, such as printer spooling
- Kernel processes, which do systemwide functions in kernel mode, such as paging

A process can run in an OpenEdition user address space, an OpenEdition forked address space, or an OpenEdition kernel address space. In an MVS system, a process is handled like a task. See also *task*. (4) An address space and one or more threads of control that execute within that address space and their required system resources. (5) An address space and single thread of control that executes within that address space and its required system resources. A process is created by another process issuing the **fork()** function. The process that issues **fork()** is known as the parent process, and the new process created by the **fork()** is known as the child process. (6) A sequence of actions required to produce a desired result. (7) An entity receiving a portion of the processor's time for executing a program. (8) An activity within the system that is started by a command, a shell program, or another process. Any running program is a process. (9) A unique, finite course of events defined by its purpose or by its effect, achieved under given conditions. (10) Any operation or combination of operations on data. (11) The current state of a program that is running—including a memory image, the program data, the variables used, the general register values, the status of opened files used, and the current directory. Programs running in a process must be either operating system programs or user programs. (12) A running program including the memory occupied, the open files, the environment, and other attributes specific to a running program.

product-sensitive programming interface (PSPI). A programming interface intended to be used only for specialized tasks such as: diagnosis, modification, monitoring, repairing, tailoring, and tuning of the IBM software product and that depends on or requires the customer to understand significant aspects of the design and implementation of the IBM software product. See also *general-use programming interface (GUPI)*.

profile. Data that describes the significant characteristics of a user, a group of users, or one or more computer resources. See also *data set profile, discrete profile, general resource profile, generic profile, group profile,* and *user profile*.

program access to data sets (PADS). A RACF function that enables an authorized user or group of users to access one or more data sets at a specified access authority only while running a specified RACF-controlled program. See also *program control*.

program control. A RACF function that enables an installation to control who can run RACF-controlled programs. See also *program access to data sets*.

PSPI. See *product-sensitive programming interface*.

R

RACF. See Resource Access Control Facility.

RACF database. A collection of interrelated or independent data items stored together without unnecessary redundancy to serve Resource Access Control Facility (RACF).

RACF remote sharing facility (RRSF). RACF services that function within the RACF subsystem address space to provide network capabilities to RACF.

RACF remove ID utility. A RACF utility which identifies references to user IDs and group IDs in the RACF database. The utility can be used to find references to residual user IDs and group IDs or specified user IDs and group IDs. The output from this utility is a set of RACF commands that can be used to remove the references from the RACF database after review and possible modification by the customer.

RACF report writer. A RACF function that produces reports on system use and resource use from information found in the RACF SMF records.

RACF SMF data unload utility. A RACF utility that enables installations to create a sequential file from the security relevant audit data. The sequential file can be used in several ways: viewed directly, used as input for installation-written programs, and manipulated with sort/merge utilities. It can also be uploaded to a database manager (for example, DB2) to process complex inquiries and create installation-tailored reports.

RACF-protected. Pertaining to a resource that has either a discrete profile, an applicable generic profile, or a file or directory that doesn't have a profile, but is protected with the File Security Packet (FSP). A data

set that is RACF-protected by a discrete profile must also be RACF-indicated.

RACROUTE macro. An assembler macro that provides a means of calling RACF to provide security functions. See also *AUDIT request, AUTH request, DEFINE request, DIRAUTH request, EXTRACT request, FASTAUTH request, LIST request, SIGNON request, STAT request, TOKENBLD request, TOKENMAP request, TOKENXTR request, VERIFY request,* and *VERIFYX request*.

remote logical unit (remote LU). See *partner logical unit (partner LU)*. These two terms are interchangeable.

remote node. An RRSF node that is logically connected to a node from whose point of view you are talking. For example, if MVSX and MVSY are two RRSF nodes that are logically connected, from MVSX's point of view MVSY is a remote node, and from MVSY's point of view MVSX is a remote node. See also *local node*, *target node*.

Resource Access Control Facility (RACF). An IBM-licensed product that provides for access control by identifying and verifying users to the system, authorizing access to protected resources, logging detected unauthorized attempts to enter the system, and logging detected accesses to protected resources.

resource profile. A profile that provides RACF protection for one or more resources. User, group, and connect profiles are not resource profiles. The information in a resource profile can include the data set profile name, profile owner, universal access authority, access list, and other data. Resource profiles can be discrete profiles or generic profiles. See *discrete profile* and *generic profile*.

root. (1) The starting point of the file system. (2) The first directory in the system. (3) See *appropriate privileges*.

RRSF. See *RACF remote sharing facility*.

RRSF logical node connection. Two RRSF nodes are logically connected when they are properly configured to communicate via APPC/MVS, and each has been configured via the TARGET command to have an OPERATIVE connection to the other.

RRSF network. Two or more RRSF nodes that have established RRSF logical node connections to each other.

RRSF node. One or more MVS system images with MVS/ESA 4.3 or later installed, RACF 2.2 installed, and the RACF subsystem address space active. See also *RRSF logical node connection*.

S

SAF. System authorization facility.

security. See *data security*.

security classification. The use of security categories, a security level, or both, to impose additional access controls on sensitive resources. An alternative way to provide security classifications is to use security labels.

SFS. Shared file system

shared file system (SFS). A part of CMS that lets users organize their files into groups known as directories and selectively share those files and directories with other users.

shell. (1) In OpenEdition MVS, a program that interprets and processes interactive commands from a pseudoterminal or from lines in a shell script. (2) A program that interprets sequences of text input as commands. It may operate on an input stream, or it may interactively prompt and read commands from a terminal. Synonymous with *command language interpreter*. (3) A software interface between a user and the operating system of a computer. Shell programs interpret commands and user interactions on devices such as keyboards, pointing devices and touch-sensitive screens and communicate them to the operating system. (4) The command interpreter that provides a user interface to the operating system and its commands. (5) The program that reads a user's commands and executes them. (6) The shell command language interpreter, a specific instance of a shell. (7) A layer, above the kernel, that provides a flexible interface between users and the rest of the system. (8) Software that allows a kernel program to run under different operating system environments.

SIGNON request. The issuing of the RACROUTE macro with REQUEST=SIGNON specified. A SIGNON request is used to provide management of the signed-on lists associated with persistent verification (PV), a feature of the APPC architecture of LU 6.2.

single-system RRSF node. An RRSF node consisting of one MVS system image.

SMF records. See *RACF SMF data unload utility*.

STAT request. The issuing of the RACROUTE macro with REQUEST=STAT specified. A STAT request determines if RACF is active and, optionally, whether a given resource class is defined to RACF and active. The STAT request replaces the RACSTAT function.

structure. See *cache structure*.

supervisor. The part of a control program that coordinates the use of resources and maintains the flow of processing unit operations. Synonym for *supervisory routine*.

supervisory routine. A routine, usually part of an operating system, that controls the execution of other routines and regulates the flow of work in a data processing system. Synonymous with *supervisor*.

syscall. In OpenEdition MVS, deprecated term for *callable service*.

sysplex. A set of MVS systems communicating and cooperating with each other through multisystem hardware elements and software services to process customer workloads.

sysplex communication. An optional RACF function that allows the system to use XCF services and communicate with other systems that are also enabled for sysplex communication.

system authorization facility (SAF). An MVS component that provides a central point of control for security decisions. It either processes requests directly or works with RACF or another security product to process them.

system call. In OpenEdition MVS, synonym for *callable service*.

T

target node. An RRSF node that a given RRSF node is logically connected to as a result of a TARGET command. The local node is a target node of itself, and all of its remote nodes are target nodes. See also *local node*, *remote node*.

task. (1) A basic unit of work to be accomplished by a computer. The task is usually specified to a control program in a multiprogramming or multiprocessing environment. (2) A basic unit of work to be performed. Some examples include a user task, a server task, and a processor task. (3) A process and the procedures that run the process. (4) In a multiprogramming or multiprocessing environment, one or more sequences of instructions treated by a control program as an element of work to be accomplished by a computer. (5) The basic unit of work for the MVS system.

TOKENBLD request. The issuing of the RACROUTE macro with REQUEST=TOKENBLD specified. A TOKENBLD request builds a UTOKEN.

TOKENMAP request. The issuing of the RACROUTE macro with REQUEST=TOKENMAP specified. A TOKENMAP request maps a token in either internal or external format, allowing a caller to access individual fields within the UTOKEN.

TOKENXTR request. The issuing of the RACROUTE macro with REQUEST=TOKENXTR specified. A TOKENXTR request extracts a UTOKEN from the current address space, task, or a caller-specified ACEE.

transaction program (TP). A program used for cooperative transaction processing within an SNA network. For APPC/MVS, any program on MVS that issues APPC/MVS or CPI Communication calls, or is scheduled by the APPC/MVS transaction scheduler.

TSO segment. The portion of a RACF profile containing TSO logon information.

U

UACC. See *universal access authority*.

UID. See *user identifier*.

universal access authority (UACC). The default access authority that applies to a resource if the user or group is not specifically permitted access to the resource. The universal access authority can be any of the access authorities.

user. A person who requires the services of a computing system.

user ID. A string of characters that uniquely identifies a user to a system. A user ID is 1 to 8 alphanumeric characters. On TSO, user IDs cannot exceed 7 characters and must begin with an alphabetic, #, $, or @ character.

user identification and verification. The acts of identifying and verifying a RACF-defined user to the system during logon or batch job processing. RACF identifies the user by the user ID and verifies the user by the password or operator identification card supplied during logon processing or the password supplied on a batch JOB statement.

user identifier (UID). (1) A unique string of characters that identifies an operator to the system. This string of characters limits the functions and information the operator can use. (2) A non-negative integer, which can be contained in an object of type *uid_t,* that is used to identify a system user. When the identity of the user is associated with a process, a user ID value is referred to as a real user ID, an effective user ID, or an (optional) saved set-user-ID. (3) The identification associated with a user or job. The two types of user IDs are:

- **RACF user ID:** A string of characters that uniquely identifies a RACF user or a batch job owner to the

security program for the system. The batch job owner is specified on the USER parameter on the JOB statement or inherited from the submitter of the job. This user ID identifies a RACF user profile.

- **OMVS user ID:** A numeric value between 0 and 2147483647, called a UID (or sometimes a user number), that identifies a user to OpenEdition services. These numbers appear in the RACF user profile for the user.

A user ID is equivalent to an account on a UNIX-type system. (4) A symbol identifying a system user. (5) Synonymous with user identification.

user name. (1) In RACF, one to 20 alphanumeric characters that represent a RACF-defined user. (2) In OpenEdition MVS, a string that is used to identify a user.

user profile. A description of a RACF-defined user that includes the user ID, user name, default group name, password, profile owner, user attributes, and other information. A user profile can include information for subsystems such as TSO and DFP. See *TSO segment* and *DFP segment*.

V

verification. See *user identification and verification*.

VERIFY request. The issuing of the RACROUTE macro with REQUEST=VERIFY specified. A VERIFY request is used to verify the authority of a user to enter work into the system. The VERIFY request replaces the RACINIT function.

VERIFYX request. The issuing of the RACROUTE macro with REQUEST=VERIFYX specified. A VERIFYX request verifies a user and builds a UTOKEN, and handles the propagation of submitter ID.

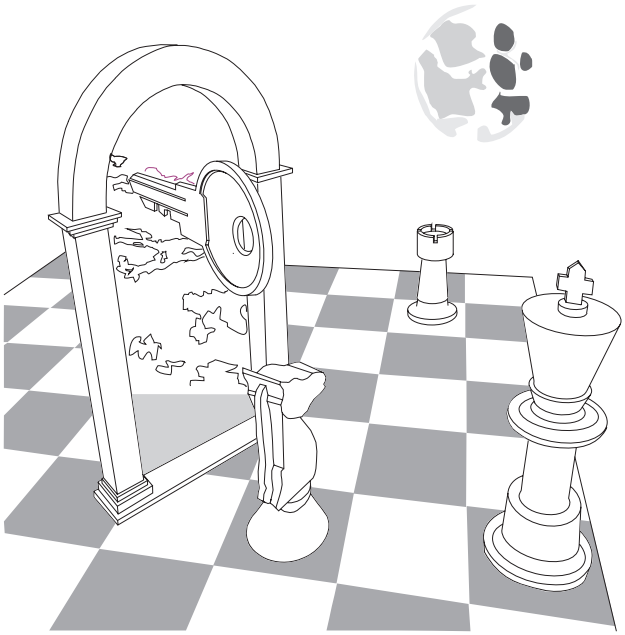
VM. A licensed program that controls “virtual machines” and runs on two main command languages, CP and CMS. Can be VM/SP, VM/HPO, VM/XA, or VM/ESA.

W

workspace data sets. VSAM data sets used by RACF for queuing requests sent to and received from target nodes in an RRSF environment.

How to Get Your RACF CD

RACF's Greatest Hits: Now on CD



Let's face it, you have to search through a ton of hardcopy manuals to locate all of the information you need to secure your entire system. There are manuals for OS/390, VM, CICS, TSO/E; technical bulletins from the International Technical Support Organization ("red books"), Washington Systems Center ("orange books"); multiple levels of OS/390 Security Server (RACF) manuals; and much more. Wouldn't it be great if you could have all of this information in one convenient package?

Now you can! The *IBM Online Library Productivity Edition OS/390 Security Server (RACF) Information Package* includes key books from a wide variety of System/390 operating system and application product libraries that refer to RACF and OS/390 Security Server (including OpenEdition DCE Security Server and RACF). You can search the information package to find all the RACF hits and hints you need.

You can view and search the books on CD-ROM at your workstation or terminal using:

- The IBM BookManager Library Reader for OS/2, DOS, or Windows**, all of which are provided at no charge with each CD-ROM
- Any of the IBM BookManager READ licensed programs for MVS, VM, OS/2, DOS, AIX/6000, or Windows.[1]

The OS/390 Security Server (RACF) Information Package is available as product feature code 8004 with OS/390 or as product feature code 9006 with RACF Version 2. You can also order it through normal publication ordering channels as SK2T-2180. If you have any specific questions or if you'd like more information about this online collection, write to us at one of the following:

- By mail, use this form. If you are mailing this form from a country other than the United States, you can give it to the local IBM branch office or IBM representative for postage-paid mailing.
- By FAX, use this number: (International Access Code)+1+914+432-9405
- IBMLink (United States customers only): KGNVMC(MHVRCFS)
- IBM Mail Exchange: USIB6TC9 at IBMMAIL
- Internet: mhvrcfs@vnet.ibm.com

Name

Company or Organization

Address

City State Zip Code

Phone or FAX Number

E-Mail Address

[1] IBM BookManager READ/MVS is part of the OS/390 product.

© Copyright IBM Corp. 1994, 1997

Index

A

access list entry
  conditional 23
  standard 23
ACEEALET keyword 16
ADDUSER command 15
administration
  classroom courses xiii
administration considerations
  migration 2
ALTUSER command 7, 13, 14, 15
application development considerations
  migration 3
auditing 23
auditing considerations
  changed SMF records 33
  migration 3
  superuser status 6

C

callable services
  changed 6, 12
  new 8, 11, 12
CDT
  see class descriptor table (CDT) 12
class descriptor table 1
  See also classes
class descriptor table (CDT)
  changes to 12
  installation-defined classes 29
  migration considerations 29
classes
  new 12
  TMEADMIN 8, 31
classroom courses, RACF xiii
commands
  ADDUSER 15
  ALTUSER 7, 13, 14, 15
  ALTUSER PASSWORD 13
  changes to 13
  PASSWORD 13
  PASSWORD USER 7
  PERMIT 8, 13, 14
  SETROPTS 10
  SETROPTS RACLIST 32
  TARGET 9, 13
compatibility
  planning considerations 23
courses on RACF xiii
CSA
  storage requirement 26
customization considerations
  class descriptor table (CDT) 29
  RACF/DB2 external security module processing 29
customizing
  migration 2

D

data areas
  changed 15
  changes for OpenEdition services 16
  changes to for new RACF FMID 16
  changes to for OpenEdition services 16
  FAST 30
  RCVT 16
  RFXP 30
  RUTKN 16
  SAFP 16
database, RACF
  templates 27
DB2 authorization
  exit point 5
DB2 external security module 5

E

ECSA
  storage requirement 27
ELSQA
  storage requirement 26
EPLPA
  storage requirement 25
ESQA
  storage requirement 26
event codes, new for SMF records 33
exits
  changes to 16, 17
  processing 30

F

FACILITY class profile 7
FLPA
  storage requirement 25
FMID 9

G

general user considerations
  migration 3

© Copyright IBM Corp. 1994, 1997

getGMAP callable service 6, 12
getUMAP callable service 6, 12
global access checking 10

H

hardware requirements
  planning considerations 22
HRF2240 9

I

ICHEACTN macro, changes to 17
ICHEINTY macro, changes to 17
ICHETEST macro, changes to 17
initUSP callable service 6, 12
installation considerations 25
  templates 27
installation exits 1
  See also exits
IRR@XACS 19
ISPF panels
  changed 19

L

library, RACF publications
  changes to 20
LOGSTR keyword 16
LSQA
  storage requirement 26

M

macros
  changes to 17
  RELEASE=2.4 keyword 17, 23
messages
  changes to 17
  new 17
migration
  recommended strategy 21
migration considerations
  administration 2
  application development 3
  auditing 3
  customization 2
  general user 3
  installation 2
  installation-defined classes 29
  overview 1
  planning 1
migration path
  from RACF 1.9 22
  from RACF 1.9.2 22
  from RACF 2.1 22
  from RACF 2.2 21
migration path *(continued)*
  from releases prior to RACF 1.9 22
  from Security Server (RACF) Release 1 21

N

new and enhanced support
  summary of changes 11

O

OpenEdition services
  auditing use of superuser status 6, 23
  changed panels 19
  changes to data areas 16
  definition of a system-wide default 6, 23
  description of enhancements 6
OS/390 OpenEdition 1
  See also OpenEdition services
OS/390 Security Server (RACF) Release 1
  migration path from 21

P

panels
  changed 19
PASSWORD command 13
password history
  changes 31
  list 31
PASSWORD USER command 7
PERMIT command 13, 14
planning considerations
  compatibility 23
  hardware requirements 22
planning for migration
  overview 1
PLPA
  storage requirement 25
PROCESS class
  auditing 23
product ID
  changes needed because of 10
program control by system ID
  administrative considerations 31
  compatibility considerations 23
program profiles 23
programming interfaces
  changes to CDT 12
  data areas 15
  new callable service 11, 12
publications
  changes to RACF library 20
  on CD-ROM xii
  softcopy xii

R

R_Admin callable service 8, 11
RACF
  classroom courses xiii
  publications
    on CD-ROM xii
    softcopy xii
RACF 1.9
  migration path from 22
RACF 1.9.2
  migration path from 22
RACF 2.1
  migration path from 22
RACF 2.2
  migration path from 21
RACF administration
  classroom courses xiii
RACF panels
  changed 19
RACF releases prior to 1.9
  migration path from 22
RACF remote sharing facility 1
  See also RRSF
RACF security topics
  classroom courses xiii
RACF/DB2 external security module 29
RACLIST keyword 10
RACROUTE macro, changes to 17
RACROUTE REQUEST=AUTH 10, 32
RACROUTE REQUEST=FASTAUTH 16, 35
RACROUTE REQUEST=LIST 10, 32
RCVT data area 16
RCVT value
  2040 9
Record Fields
  SMF80DA2 33
  SMF80DTA 33
RELEASE=2.4 keyword on macros 17, 23, 35
remote sharing 1
  See also RRSF
router table
  installation-defined classes 29
RRSF local nodes 9
run-time library services
  overview 7
RUTKN data area 16

S

SAFP data area 16
Security Server (RACF) Release 1
  migration path from 21
security topics for RACF
  classroom courses xiii
SETROPTS command 10
SETROPTS RACLIST command 32
SMF records
  changes to 23, 33
SMFID 8
spawn service
  auditing 6
SQA
  storage requirement 25
storage for RACF
  virtual 25
storage requirement
  virtual for RACF 25
superuser status
  auditing 6
SYS1.SAMPLIB
  change for DB2 authorization support 19
system identifier 8
system-wide default
  for OpenEdition segment information 6

T

TARGET command 9, 13
TARGET command enhancements 9
templates
  installation considerations 27
TMEADMIN class 8

U

user private, below 16MB
  storage requirement 27

V

virtual storage requirement for RACF 25
virtual storage usage for RACF 25

W

WDSQUAL keyword on TARGET command 9

Readers' Comments — We'd Like to Hear from You

OS/390
Security Server (RACF)
Planning: Installation and Migration

Publication No. GC28-1920-03

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	□	□	□	□	□

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	□	□	□	□	□
Complete	□	□	□	□	□
Easy to find	□	□	□	□	□
Easy to understand	□	□	□	□	□
Well organized	□	□	□	□	□
Applicable to your tasks	□	□	□	□	□

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? □ Yes □ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name _____ Address _____

Company or Organization _____

Phone No. _____

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Department 55JA, Mail Station P384
522 South Road
Poughkeepsie, NY 12601-5400

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold
Along Line

Program Number: 5647-A01

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

GC28-1920-03